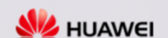
# 华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*) 享有如下特权：

- 1、华为E-learning 课程学习
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：请提交您的“华为账号”和注册账号的“email地址”到 *Learning@huawei.com 申请权限。*
- 2、华为培训教材下载
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训->面授培训*”，在具体课程页面即可下载教材。
- 3、华为在线公开课(LVC)优先参与
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见LVC排期：
    http://support.huawei.com/learning/NavigationAction!createNavi#navi[id]=_16
- 4、学习工具 eNSP
  - *eNSP (Enterprise Network Simulation Platform),* 是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。（http://support.huawei.com/ecommunity/bbs/list_2247.html ）






HC120310001
防火墙高级设备管理
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



# 目标

- 学完本课程后，您将能够:
  - 熟悉防火墙基础管理方式
  - 掌握使用AAA方式管理防火墙
  - 掌握处理密码故障









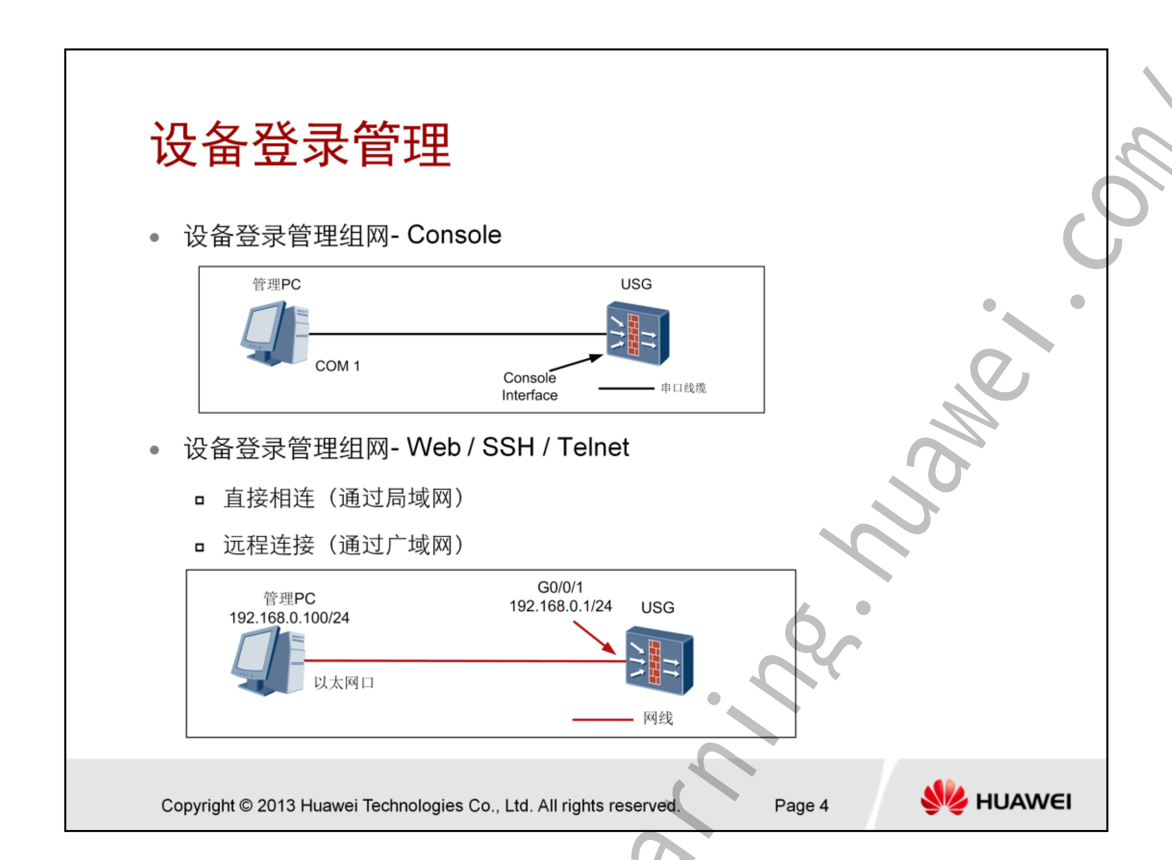
# 目录












通过Console口登录:

使用PC终端通过连接设备的Console口来登录设备，进行第一次上电和配置。当用户无法进行远程访问设备时，可通过Console进行本地登录；当设备系统无法启动时，可通过console口进行诊断或进入BootRom进行系统升级。

通过Telnet登录:

通过PC终端连接到网络上，使用Telnet方式登录到设备上，进行本地或远程的配置，目标设备根据配置的登录参数对用户进行验证。Telnet登录方式方便对设备进行远程管理和维护。

通过SSH登录:

提供安全的信息保障和强大认证功能，保护设备系统不受IP欺骗、明文密码截取等攻击。SSH登录能更大限度的保证数据信息交换的安全。

通过Web登录:

在客户端通过Web浏览器访问设备，进行控制和管理。适用于配置终端PC通过Web方式登录。

注意：PC和USG以太网口的IP地址必须在同一网段或PC和USG之间有可达路由。

# 通过Console口登录设备

- USG配置口登录的缺省用户名为admin，缺省用户密码为Admin@123。其中，用户名不区分大小写，密码要区分大小写。











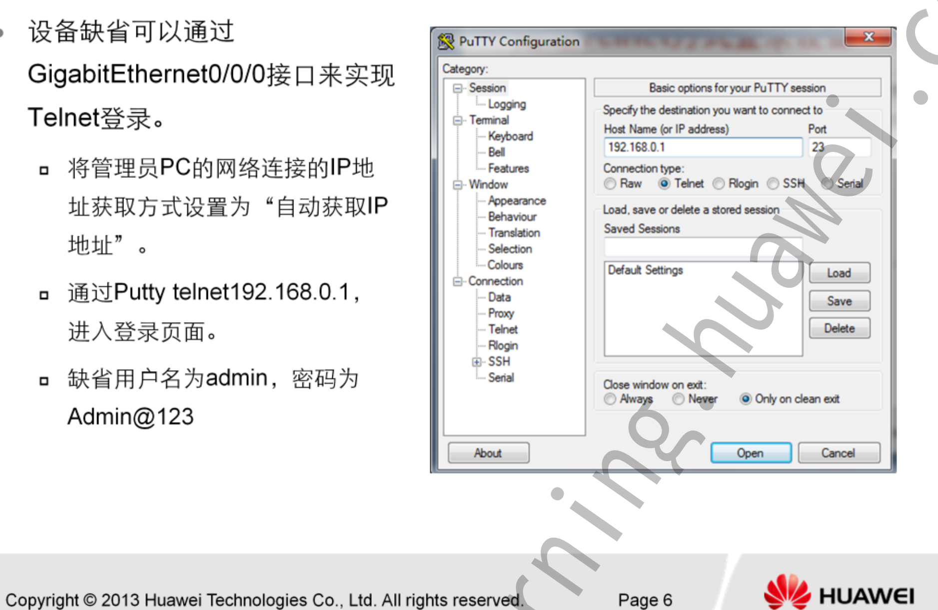

通过Console口登录:

使用PC终端通过连接设备的Console口来登录设备，进行第一次上电和配置。当用户无法进行远程访问设备时，可通过Console进行本地登录；当设备系统无法启动时，可通过console口进行诊断或进入BootRom进行系统升级。

如果使用PC进行配置，需要在PC上运行终端仿真程序（如Windows3.1的Terminal，Windows98/Windows2000/Windows XP的超级终端），建立新的连接。如图所示，键入新连接的名称，单击“确定”。

在串口的属性对话框中设置波特率为9600，数据位为8，奇偶校验为无，停止位为1，流量控制为无，单击“确定”，返回超级终端窗口。

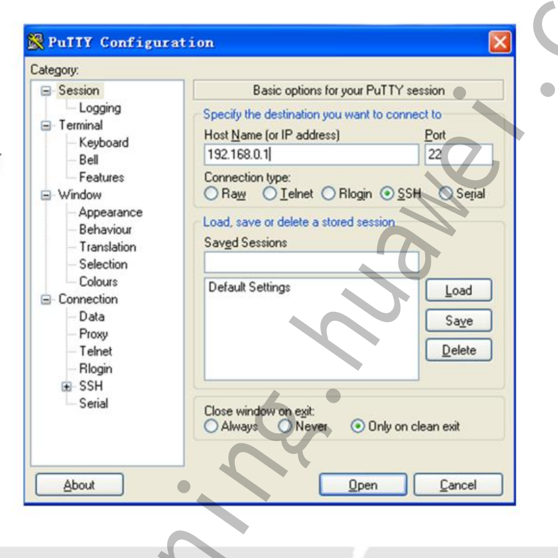
打开设备电源开关。设备上电后，检查设备前面板上的指示灯显示是否正常。




GigabitEthernet 0/0/0接口加入Trust域并提供缺省IP地址（192.168.0.1/24），并开放Trust域到Local域的缺省包过滤，方便初始登录设备。

## 通过SSH方式登录设备

- 设备可以通过GigabitEthernet0/0/0接口来实现SSH登录。
  - 使用Telnet或Console口登陆方式登陆设备，启用Stelnet服务。
  - 通过Putty SSH192.168.0.1，进入登录页面。
  - 缺省用户名为admin，密码为Admin@123








HUAWEI

SSH可以为用户登录设备系统提供安全的信息保障和强大的认证功能。配置USG接口SSH设备管理，管理员根据实际的需要打开。

在USG上生成本地密钥对。

成功完成SSH登录的首要操作是：配置并产生本地RSA密钥对。请您在进行其它SSH配置之前，一定记得完成rsa local-key-pair create配置，生成本地密钥对。此命令只需执行一遍，设备重启后不必再次执行。

在USG上创建SSH用户。

设备作为SSH服务器时，可配置对SSH用户的验证方式为Password、RSA方式。

启用USG的服务方式为STelnet/SFTP服务。

执行命令ssh user user-name service-type { sftp | stelnet | all }，为SSH用户配置服务方式。

在使用SSH1.5版本配置SSH终端服务时，不需进行该配置；在使用SSH2.0版本配置SSH终端服务时，必须配置该命令。

启用USG的STelnet/SFTP服务。

配置SSH服务器功能。 执行命令stelnet server enable，启用Stelnet服务。

在使用SSH1.5版本配置SSH终端服务时，不需进行该配置；在使用SSH2.0版本配置SSH终端服务时，必须配置该命令。

## 通过Web方式登录设备

- 设备缺省可以通过GigabitEthernet0/0/0接口来登录Web界面。
  - 将管理员PC的网络连接的IP地址获取方式设置为“自动获取IP地址”。
  - 将PC的以太网口与设备的缺省管理接口直接相连，或者通过交换机中转相连。
  - 在PC的浏览器中访问http://192.168.0.1，进入Web界面的登录页面。
  - 缺省用户名为admin，密码为Admin@123








缺省情况下，设备开启HTTP；建议开启HTTPS，提高安全性。用户可以通过用户名/密码：admin/Admin@123登录，为保证系统安全，登录后请修改密码。

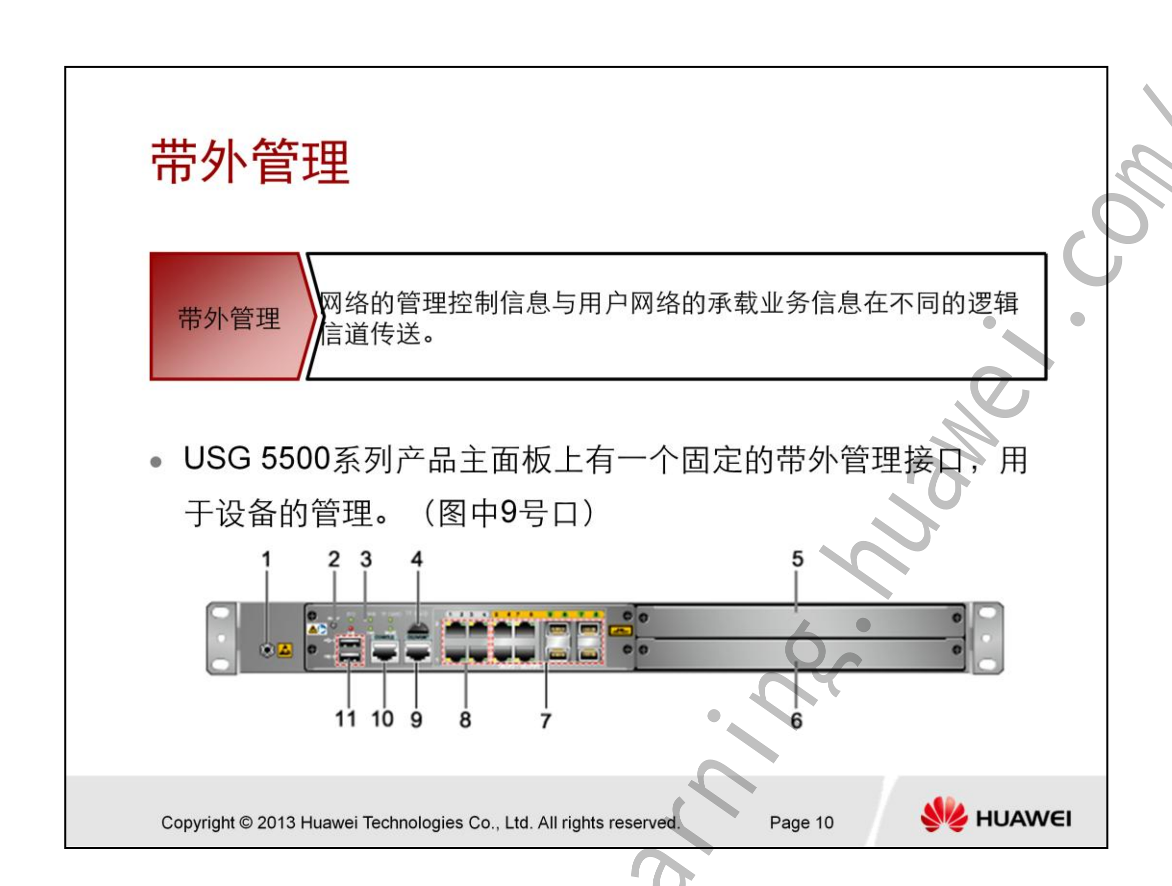
只有GigabitEthernet 0/0/0接口加入Trust域并提供缺省IP地址（192.168.0.1/24），并开放Trust域到Local域的缺省包过滤，方便初始登录设备。

缺省情况下开放Local域到其他任意安全区域的缺省包过滤，方便设备自身的对外访问。

其他接口都没有加安全区域，并且其他域间的缺省包过滤关闭。要想设备转发流量必须将接口加入安全区域，并配置域间安全策略或开放缺省包过滤。




在缺省情况下，在USG中低端系列产品中，GE0/0/0拥有一个缺省IP地址192.168.0.1/24用作设备管理。并开启web管理功能和接口DHCP服务。此接口可作为设备的带内管理接口。




带外管理接口作为一个逻辑信道单独传送管理控制信息。

# 文件系统

- 文件系统由储存设备和保存在储存设备的文件组成，可实现管理存储设备、管理保存在存储设备中的文件两类功能。
- USG系列防火墙对文件的操作主要有以下几类：

| 管理存储设备 | |
|---|---|
| 管理项目 | 命令 |
| 修复文件系统异常的存储设备 | fixdisk |
| 格式化存储设备 | format |

| 管理目录/文件 | |
|---|---|
| 管理项目 | 命令 |
| 恢复删除文件 | undelete |

| 管理目录/文件 | | | |
|---|---|---|---|
| 管理项目 | 命令 | 管理项目 | 命令 |
| 创建目录 | mkdir | 显示文件的内容 | more |
| 重新命名目录 | rename | 拷贝文件 | copy |
| 查看当前的工作目录 | pwd | 移动文件 | move |
| 改变当前目录 | cd | 重新命名文件 | rename |
| 显示目录或文件信息 | dir | 压缩文件 | zip |
| 删除目录 | rmdir | 删除文件 | delete |
| 执行批处理文件 | execute | 彻底删除回收站中的文件 | reset |



HUAWEI

文件系统是指对存储设备中的文件、目录的管理，包括创建文件系统，创建、删除、修改、更名文件和目录，以及显示文件的内容。包括以下部分：

存储设备：是指存储文件的硬件设备，本产品目前支持的存储设备为闪存卡。

文件：是系统存储信息的个体，通过对文件的操作来实现对信息的管理。

目录：是文件的一个整体集合，是文件的逻辑上的容器。




如图所示，在对防火墙配置文件进行管理时，可直接点击“选择”，查看到设备上已保存的配置文件，对其进行删除、修改、应用等操作。也可点击“上传”，上传一个新的配置文件。




设备启动时会读取配置文件进行系统的初始化工作，该配置文件中的配置称为启动配置。与启动配置相对应，设备运行过程中正在生效的配置称为当前配置。用户对设备所做的修改会即时生效，但不会自动保存到配置文件中，这些修改在设备断电后会丢失，所以在完成所有修改后请使用**save**命令保存配置。本节所做的备份和恢复工作针对的是配置文件，需要重启后才会生效。

- 使用FTP/TFTP服务器备份和恢复配置文件（推荐）

需要配置FTP/TFTP软件，将配置文件保存在服务器上。适用于较多设备的配置集中维护的情况。

- 设备作为FTP服务器备份和恢复配置

不需要配置FTP软件，不过需要在设备上配置FTP Server功能。开放FTP端口会给设备带来一定的安全隐患。

- 将配置文件备份在设备的存储器上

操作简单，不需要安装其他软件。如果备份在相同存储介质上，可能导致主用和备份配置文件同时损坏。

- 通过Web备份和恢复配置

操作简单，需要提前完成web登录的配置。通常适用于桌面型接入网关。

## 备份与恢复配置文件举例 - CLI

- 设备做FTP Server。首先启用FTP功能并设置FTP密码及路径。然后使用get/put命令下载或上传文件。

[USG] **ftp server enable**

Info:Start FTP server

[USG] **aaa**

[USG -aaa] **local-user ftpuser password simple Ftppass#**

[USG -aaa] **local-user ftpuser service-type ftp**

[USG -aaa] **local-user ftpuser ftp-directory hda1:/**








**local-user ftp-directory**命令用于配置FTP路径，该路径为设备收到文件的保存路径。


备份与恢复配置文件举例 - Web
可通过从本地上传配置文件来恢复配置文件。
系统
维护
配置管理
配置文件管理
上传
删除
刷新
文件名
文件大小(字节)
最后修改时间
状态
配置
下载
flash:/ssl_vpn_cfg.zip
1747
2011/09/29 12:22:56
flash:/vrpcfg.zip
0
2013/11/20 20:09:15
flash:/1.zip
1236
2013/05/22 15:03:24
flash:/samoa.cfg
5062
2013/11/04 13:55:54
返回
可通过下载配置文件到本地对该文件进行备份。
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 15
HUAWEI

## 版本升级操作 - CLI

- 升级系统文件

```
[USG] startup system-software V300R001C00SPC100.bin
```

- 升级补丁文件

```
[USG] patch load patch.pat
[USG] patch active patch.pat
[USG] patch run patch.pat
```







无论是对系统文件还是补丁文件进行操作时，都需要先将文件用FTP或其他方式将文件上传至设备存储中。

采用命令行对系统文件进行升级时，需运行**reboot**命令重启设备才能生效。系统软件必须以“.bin”作为扩展名，且不支持中文。

**patch load**命令用来加载补丁。加载补丁时，系统会自动对该补丁进行校验，以验证该补丁和主机版本的校验和是否一致，如果不一致，补丁将加载失败，但是补丁文件名还在（只要原补丁处于运行状态）。

**patch active**命令用来激活处于非激活状态的补丁。使用该命令时，如果补丁不存在将提示失败。 补丁被激活后，并没有生效，还需要对其进行运行操作。 激活态的补丁在系统重启后将恢复为非激活态。

**patch run**命令用来运行补丁。使用该命令时，被运行的补丁必须处于激活态。 如果补丁不存在或处于去激活态将提示失败。如果设备的补丁未被删除，系统重新启动后，只有运行态的补丁会自动恢复。

对补丁文件的操作命令还有**patch deactive**以及**patch delete**。**patch deactive**命令用于去激活补丁。**patch delete**命令用来删除补丁。执行此命令后，不论补丁处于任何状态，都将被删除。

对补丁文件的操作不需要重启设备即可生效。

## 版本升级操作 - Web

在线升级分为通过内网服务器升级或通过安全服务中心升级。

在线升级

升级后保存新的知识库文件 ☑ 启用

自动升级周期 90 <1-365>天 手动在线升级

本地升级

文件 选择

本地升级

当设备无法访问安全服务中心时，可以进行本地升级。





HUAWEI

在web界面下对设备系统文件的操作更为方便快捷。在“系统 > 维护 > 系统更新”中，可完成对系统文件和补丁文件的升级/一键升级。

在线升级分为通过内网服务器升级或通过安全服务中心升级： 通过内网服务器：指在内网部署一台升级服务器，定期从安全服务中心下载库文件，并保存在HTTP服务器根目录下。普通PC通过访问升级服务器完成升级。此时，升级服务器上需要配置LUS（Live Update Server）。有关LUS的配置过程，请参见LUS的帮助。

通过安全服务中心升级：指设备连接到安全服务中心下载病毒库和IPS签名库。



# 目录

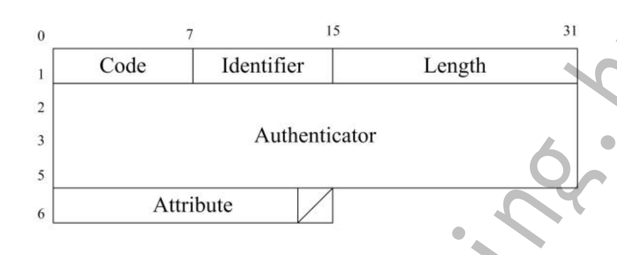







# Radius方式介绍

- Radius 协议实现
  - RADIUS使用UDP（User Datagram Protocol）作为传输协议，具有良好的实时性；同时也支持重传机制和备用服务器机制，从而具有较好的可靠性。
- RADIUS的消息结构如图所示











AAA可以用多种协议来实现，最常用的是RADIUS协议。RADIUS广泛应用于网络接入服务器NAS（Network Access Server）系统。NAS负责把用户的认证和计费信息传递给RADIUS服务器。RADIUS协议规定了NAS与RADIUS服务器之间如何传递用户信息和计费信息以及认证和计费结果，RADIUS服务器负责接收用户的连接请求，完成认证，并把结果返回给NAS。

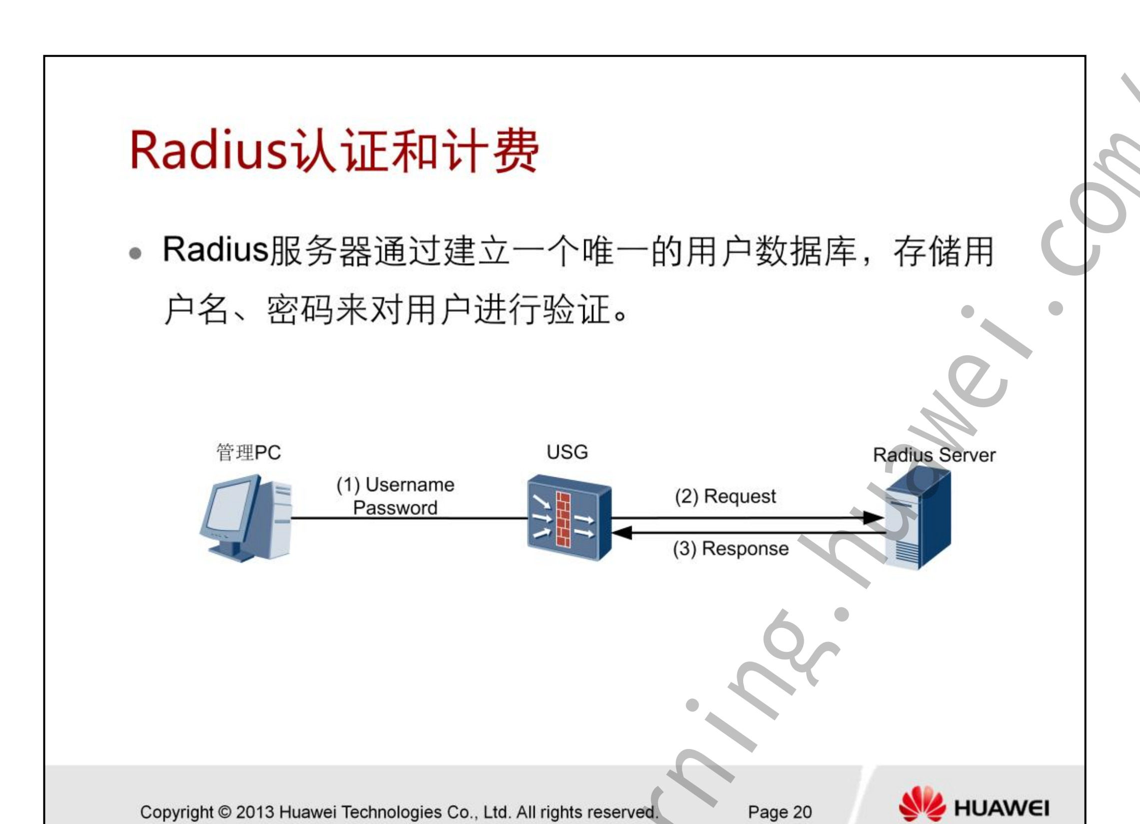
RADIUS的实现比较简单，适用于大用户量时服务器端的多线程结构。

网络接入服务器作为RADIUS协议的客户端，可以实现标准RADIUS协议及扩充属性，包括RFC2865、RFC2866，以及华为扩展的私有属性。

计费结束报文的本地缓存重传功能：计费结束报文在重传发送失败次数超过配置次数后，将计费结束报文保存到计费结束报文缓存队列；系统定时器周期扫描该队列，如果存在计费结束缓存报文，则取出报文内容，向指定的服务器发送并启动定时器等待，如果发送失败或在超时时间内没有收到服务器回应，则重新入缓存队列。

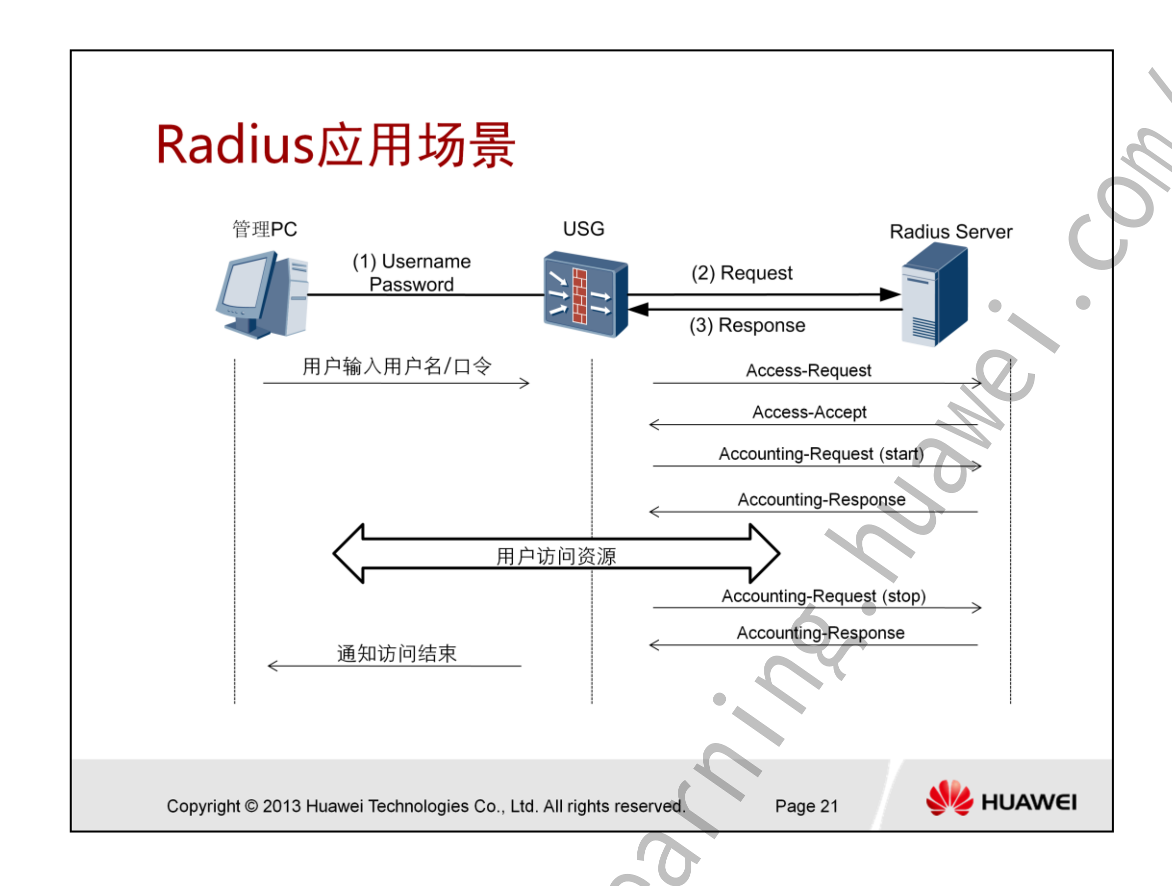
Radius协议中各字段的含义简单说明如下：

- Code：消息类型，如接入请求、接入允许等。
- Identifier：一般是顺序递增的数字，请求报文和响应报文中该字段必须匹配。
- Length：所有域的总长度。
- Authenticator：验证字，用于验证RADIUS的合法性。
- Attribute：消息的内容主体，主要是用户相关的各种属性。




RADIUS客户端与服务器间的消息流程如下：

1. 用户登录USG或接入服务器等网络设备时，会将用户名和密码发送给该网络接入服务器；
2. 该网络设备中的RADIUS客户端（网络接入服务器）接收用户名和密码，并向RADIUS服务器发送认证请求；
3. RADIUS服务器接收到合法的请求后，完成认证，并把所需的用户授权信息返回给客户端；对于非法的请求，RADIUS服务器返回认证失败的信息给客户端。




Radius报文交互流程如下：

1. 用户输入用户名密码
2. 认证请求
3. 认证接受
4. 计费开始请求
5. 计费开始请求响应报文
6. 用户访问资源
7. 计费结束请求报文
8. 计费结束请求响应报文
9. 访问结束

Code为包类型。包类型占1个字节，定义如下：

- Access-Request——请求认证过程
- Access-Accept——认证响应过程
- Access-Reject——认证拒绝过程
- Accounting-Request——请求计费过程
- Accounting-Response——计费响应过程
- Access-Challenge ——访问质询

## Radius配置实例 （CLI）

- 配置RADIUS服务器主要包括新建RADIUS服务器模板，在模板视图下指定认证、授权、计费服务器的IP地址，以及调整RADIUS服务器的参数。
- 在AAA配置中配置当前域的RADIUS服务器模板。所指向的RADIUS服务器模板必须已经配置完成并存在。

[USG] **aaa**

[USG -aaa] **domain domain1**

[USG -aaa-domain-domain1] **radius-server server**








Radius 服务器模板配置举例：

[USG] **radius-server template server**

[USG-radius-server] **radius-server authentication 1.1.1.1 1812**

[USG-radius-server] **radius-server authentication 2.2.2.2 1812 secondary**

[USG-radius-server] **radius-server accounting 1.1.1.1 1645**

[USG-radius-server] **radius-server accounting 2.2.2.2 1645 secondary**

[USG-radius-server] **radius-server shared-key abcde**

[USG-radius-server] **radius-server retransmit 4**

[USG-radius-server] **radius-server timeout 6**

# Radius配置实例 （WEB）

用户 > 认证服务器 > RADIUS服务器

**新建RADIUS服务器**

| | | | |
|---|---|---|---|
| RADIUS服务器名称 | RadiusServer * | 共享密钥 | •••••• |
| 认证主服务器IP | 1 . 1 . 1 . 1 | 端口 | 1812 <1-65535> |
| 认证从服务器IP | 2 . 2 . 2 . 2 | 端口 | 1812 <1-65535> |
| 计费主服务器IP | 1 . 1 . 1 . 1 | 端口 | 1645 <1-65535> |
| 计费从服务器IP | 2 . 2 . 2 . 2 | 端口 | 1645 <1-65535> |

**高级选项**

| | | | |
|---|---|---|---|
| 重传次数 | 4 | 字节格式 | Byte |
| 应答超时时间 | 6 秒 | 服务器类型 | ◉ 标准 ○ Portal |
| NAS-Port端口类型 | ○ 旧 ◉ 新 | NAS-Port-Id端口类型 | ○ 旧 ◉ 新 |
| 计费停止报文重传 | ☐ 启用 | | |
| 用户名格式 | ☐ 包含用户组名称 | | |

应用 检测 返回

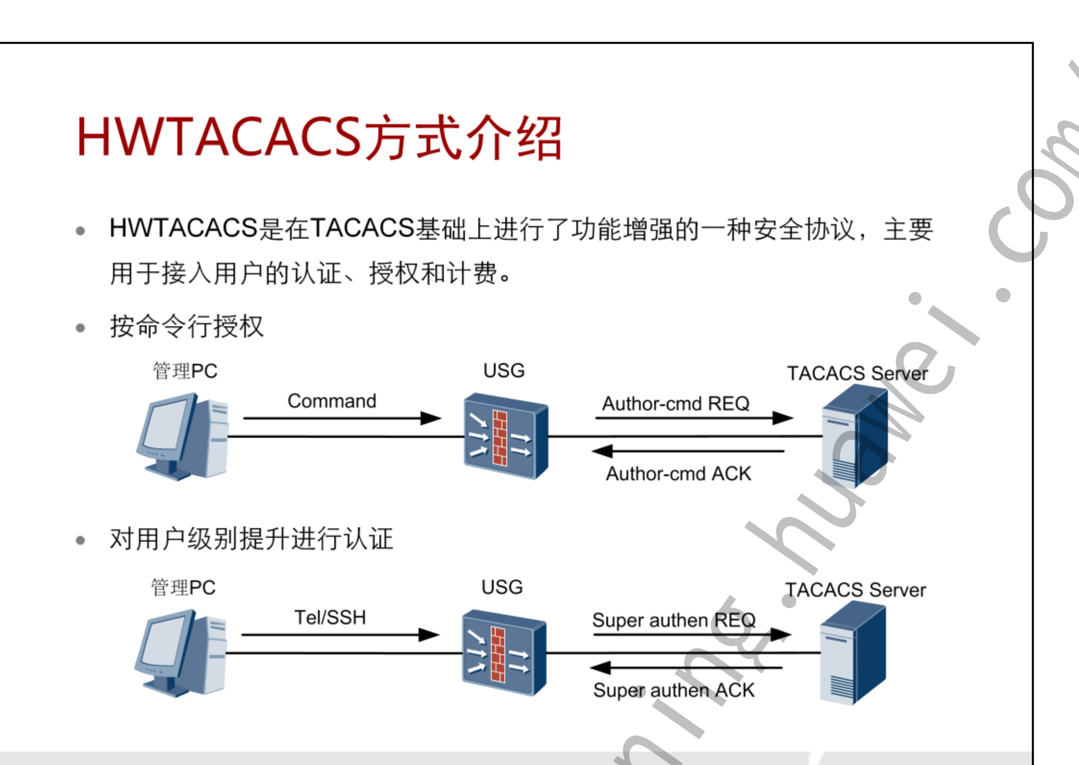






在Web配置界面中，配置Radius服务器的操作步骤如下:

1. 选择“用户 > 认证服务器 > RADIUS服务器”。
2. 单击“RADIUS服务器列表”的“新建”。
3. 依次输入或选择各项参数。
4. 单击“应用”。




**按命令行授权**

用户通过Telnet或者SSH登录到USG上后，如果需要对该用户输入的命令行进行认证，可以将该级别用户的命令行授权方法设置为HWTACACS，该用户输入的每一条命令都要通过HWTACACS服务器授权。如果授权通过，命令就可以被执行。否则，HWTACACS服务器输出信息，通知用户该命令的授权失败，命令不能执行。

命令行授权可以使用本地授权的方法作为备选方法，这样，如果因为服务器的问题（服务器Down、不可达或回应超时）导致命令行授权失败时，可以将命令行授权转入本地授权处理。

如果在用户配置的超时时间内，USG没有接收到HWTACACS服务器的授权结果，则授权超时，该命令不能被执行。

用户还可以配置服务器无响应或本地未配置用户时命令授权失败的策略，可以选择让用户继续在线，也可以选择授权失败次数超过阈值后下线。

**对用户级别提升进行认证**

用户通过Telnet或者SSH登录到USG后，可以通过在用户模式下使用**super**命令来提升自己的级别。这时，USG对用户的密码进行验证。

HWTACACS可以对用户级别的提升进行认证，其执行流程如图所示。USG将用户的密码发送到HWTACACS服务器上进行认证，如果认证通过，用户的权限就可以得到提升，否则，用户的权限不能提升。特权等级更改的结果只影响本次登录。

# HWTACACS协议和RADIUS协议的比较

| | HWTACACS | RADIUS |
|---|---|---|
| 端口使用 | 使用TCP协议，网络传输更可靠 | 使用UDP协议。认证和授权端口号是1812和1813，或者1645和1646. |
| 加密情况 | 除了标准的HWTACACS报文头，对报文主体全部进行加密 | 只是对认证报文中的密码字段进行加密 |
| 认证和授权 | 认证与授权分离 | 认证与授权一起处理 |
| 应用 | 适于进行安全控制 | 适于进行计费 |
| 配置命令授权 | 支持对配置命令进行授权 | 不支持对配置命令进行授权 |






RADIUS相比，HWTACACS具有更加可靠的传输和加密特性，更加适合于安全控制。HWTACACS协议与RADIUS协议的主要区别如表格所示。

# HWTACACS配置实例 (CLI)

- 配置HWTACACS服务器主要包括新建HWTACACS服务器模板，在模板视图下指定认证、授权、计费服务器的IP地址，以及调整HWTACACS服务器的参数。
- 配置HWTACACS服务器也需要在AAA配置中配置当前域的HWTACACS服务器模板。

[USG] **aaa**

[USG -aaa] **domain domain1**

[USG -aaa-domain-domain1] **hwtacacs-server server1**








HWTACACS 服务器模板配置举例:

[USG] **hwtacacs-server template server1**

[USG-hwtacacs-server1] **hwtacacs-server authentication 3.3.3.3 10000**

[USG-hwtacacs-server1]**hwtacacs-server authentication 4.4.4.4 10000 secondary**

[USG -hwtacacs-server1] **hwtacacs-server authorization 3.3.3.3 10005**

[USG -hwtacacs-server1] **hwtacacs-server authorization 4.4.4.4 10005 secondary**

[USG -hwtacacs-server1] **hwtacacs-server accounting 3.3.3.3 10010**

[USG -hwtacacs-server1] **hwtacacs-server accounting 4.4.4.4 10010 secondary**

# HWTACACS配置实例 (WEB)

用户 > 认证服务器 > HWTACACS服务器

新建HWTACACS服务器

| | | | |
|---|---|---|---|
| HWTACACS服务器名称 | hwtacacsServer * | 共享密钥 | |
| 认证主服务器IP | 3 . 3 . 3 . 3 | 端口 | 10000 <1-65535> |
| 认证从服务器IP | 4 . 4 . 4 . 4 | 端口 | 10000 <1-65535> |
| 授权主服务器IP | 3 . 3 . 3 . 3 | 端口 | 10005 <1-65535> |
| 授权从服务器IP | 4 . 4 . 4 . 4 | 端口 | 10005 <1-65535> |
| 计费主服务器IP | 3 . 3 . 3 . 3 | 端口 | 10010 <1-65535> |
| 计费从服务器IP | 4 . 4 . 4 . 4 | 端口 | 10010 <1-65535> |

高级选项

| | | | |
|---|---|---|---|
| 源IP地址 | . . . | 字节格式 | Byte |
| 应答超时时间 | 5 <1-30>秒 | 恢复激活时间 | 5 <1-255>分钟 |
| 用户名格式 | ☑ 包含用户组名称 | | |

应用 返回





HUAWEI

在Web配置界面中，配置HWTACACS服务器的操作步骤如下:

1. 选择“用户 > 认证服务器 > HWTACACS服务器”。
2. 单击“HWTACACS服务器列表”的“新建”。
3. 依次输入或选择各项参数。
4. 单击“应用”。



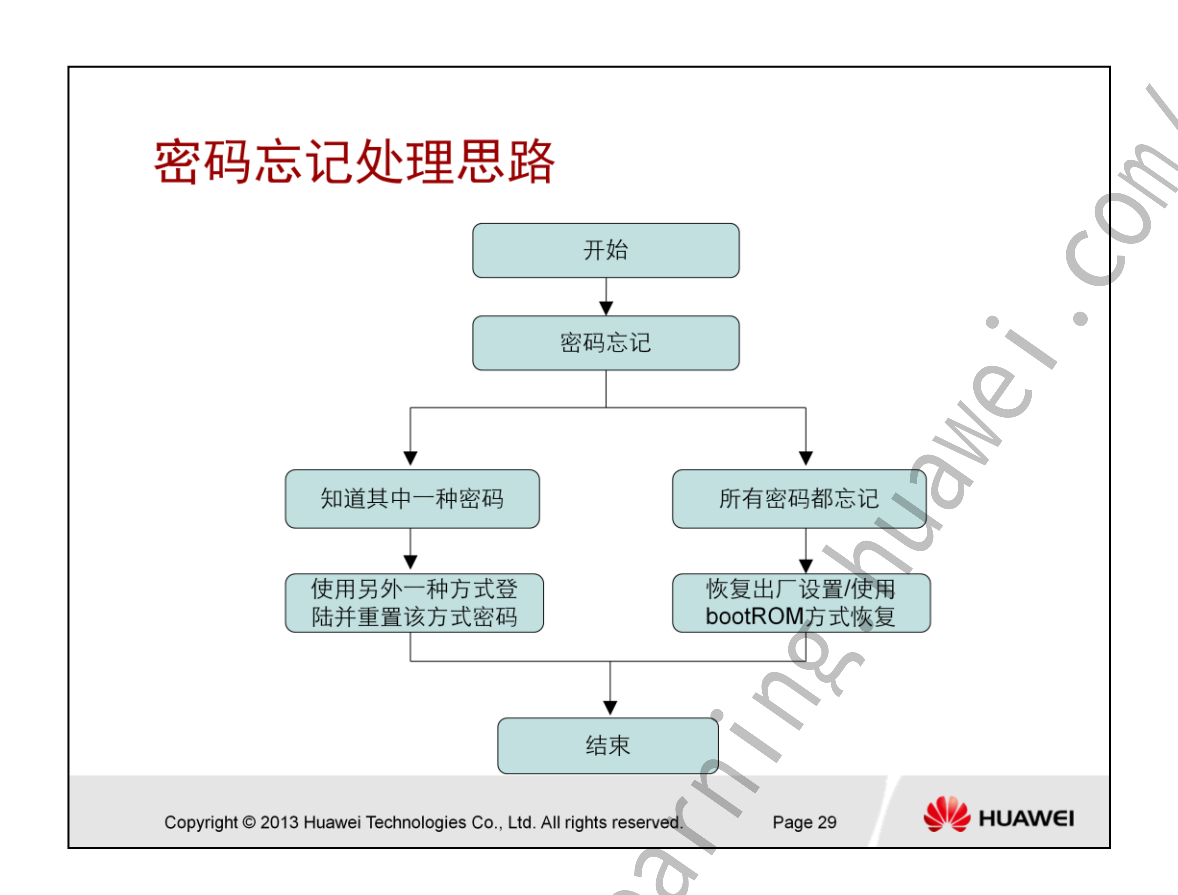
# 目录










密码忘记处理思路
开始
密码忘记
知道其中一种密码
所有密码都忘记
使用另外一种方式登
陆并重置该方式密码
恢复出厂设置/使用
bootROM方式恢复
结束
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 29
HUAWEI

# Telnet登陆密码遗忘 （1）

- AAA方式：使用用户名+密码方式登录。

```
[USG] user-interface vty 0 4
[USG -ui-vty0-4] authentication-mode aaa
[USG] aaa
[USG -aaa] local-user admin1 password cipher Admin@123
[USG -aaa] local-user admin1 service-type telnet
[USG -aaa] local-user admin1 level 15
```

- 该配置完成后用户可以使用用户名“admin1”，密码“Admin@123”登录设备。






Telnet协议可以对设备进行远程维护和管理，如果Telnet密码丢失，只能通过其他方式登录设备后重新进行配置。

用户的密码保存方式分为cipher和simple两种，在配置密码时必须选择其中一种。如果用户配置为simple方式，使用**display current-configuration configuration user-interface**命令可以直接查看配置的密码。如果使用的是cipher方式则看到的是加密后的密文，无法直接阅读。

# Telnet登陆密码遗忘 （2）

- Password方式：只使用密码登录。

```
[USG] user-interface vty 0 4
[USG -ui-vty0-4] authentication-mode password
[USG -ui-vty0-4] set authentication password cipher Admin@123
[USG -ui-vty0-4] user privilege level 15
```

- 该配置完成后用户可以输入密码 “Admin@123”登录设备。





# Telnet登陆密码遗忘 （3）

- None方式：不需要验证即可登录。

```
[USG] user-interface vty 0 4
[USG -ui-vty0-4] authentication-mode none
[USG -ui-vty0-4] user privilege level 15
```

- 该配置完成后，不需要用户名和密码就可以登录设备。





## Console密码忘记 （1）

- 在BootROM中配置跳过Console口密码登录后，重新进行设置:
  1. 重启设备，出现 “Press Ctrl+B to Enter Boot Menu...”打印信息时，按下 “Ctrl+B”并键入密码 “O&m15213”后进入BootROM主菜单。
  2. 在主菜单中或隐藏菜单（主菜单中按Ctrl+z进入）中选择 “Recover Console Password”对应序号。
  3. 在主菜单中选择 “Reboot”重新启动。
  4. 进入系统后，配置Console口用户名及密码。
  5. 保存修改，重启后可以使用新的用户名和密码登录。








部分设备的BootROM提供了清空Console口密码的功能，可以在用户使用Console口登录的时候跳过用户名密码检查。这样系统启动后除了不需要输入console密码外，与正常启动相同，也会完成所有配置加载。

请注意，要进入到BootROM菜单需要重启设备，会导致业务中断，请视具体情况做好设备备份，并尽量选择业务量较少的时间操作。清空Console口密码登录后请马上配置新的密码，否则登录超时或重启后，仍需要清空密码来登录。

在第二步中，部分设备显示为 “Skip Console0 Password”，该选项功能作用与 “Recover Console Password”作用相同。如果主菜单和隐藏菜单均没有类似选项，则说明设备不支持跳过Console口密码登录，请选择其他方法解决。

## Console密码忘记 （2）

- 使用 “Reset”键采用缺省配置启动后，修改Console口密码：
  1. 按住设备的 “Reset”键，打开电源开关。当面板指示灯以2Hz频率一起闪烁的时候，松开 “Reset”键。
  2. 完成启动后，设备会恢复为默认的出厂配置。
  3. 配置设备为FTP Server。
  4. 查看目前设备使用的启动配置文件。可以看到下次启动使用的配置文件为hda1:/vrpcfg.cfg
  5. 从PC上下载设备上的配置文件。
  6. 在PC上使用文本编辑工具修改配置文件内容，将VTY认证部分修改为none。保存后关闭。
  7. 将修改后的配置文件上传回设备，并覆盖原有配置文件。
  8. 重启设备，选择不保存配置。
  9. 设备完成启动后，Console口登录不需要密码。







如果设备的BootROM没有提供清空Console口密码功能，可以使用 “Reset”键采用缺省配置进行启动。启动后将配置文件导出并修改Console口密码，覆盖回设备上的配置文件，达到修改登录密码的效果。

FTP server配置参考命令：

[USG] **ftp server enable**

[USG] **aaa**

[USG -aaa] **local-user ftpuser password simple Ftppass#**

[USG -aaa] **local-user ftpuser service-type ftp**

[USG -aaa] **local-user ftpuser ftp-directory hda1:/**

查看下次启动使用的配置文件，使用 display startup命令。

在第七步中，如果使用备份的配置文件覆盖回设备，则可以实现配置恢复功能。



# 总结

- 防火墙基础管理方式
- 使用AAA方式管理防火墙
- 处理密码故障的方式






## 思考题

- 基本的防火墙管理方式有哪些?
- Radius 和HWTACACS有哪些区别?
- 管理忘记密码应该怎么处理?







基本的防火墙管理方式有哪些?

答题要点：Console、Telnet、SSH、HTTP等。

Radius 和HWTACACS有哪些区别?

答题要点：从端口使用、加密情况、认证和授权、应用、配置命令授权进行分析。

管理忘记密码应该怎么处理?

答题要点：首先确认是所有密码均忘记还是只忘记其中一种密码。忘记其中一种方式可采用已知的另外的方式恢复。忘记所有的可选择bootROM等方式恢复。

## 练习题

- 基本的防火墙管理方式有哪些?
- Radius 和HWTACACS有哪些区别?
- 管理忘记密码应该怎么处理?




习题与答案:

1. 报文分片处理机制中的分片丢弃是指防火墙收到攻击报文时，对报文进行分片后丢弃。

   答案：错误

2. DHCP Snooping攻击防范技术，包括以下哪些?

   A. DHCP Server仿冒者攻击

   B.中间人攻击与IP/MAC Spoofing攻击

   C.改变CHADDR值的DoS攻击

   D. DHCP Client仿冒者攻击

   答案：A|B|C

Thank you

www.huawei.com


HC120310002
防火墙高级安全特性
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



# 目标

- 学完本课程后，您将能够:
  - 理解防火墙限流策略原理与配置
  - 理解防火墙负载均衡原理与配置








# 目录

1. **防火墙限流策略**
2. 防火墙负载均衡原理







## 流量限制

**IP连接数限制**

对指定IP或者网络发起的连接数量或接收的连接数量进行限制。

**IP带宽限制**

对指定IP或者网络的会话带宽进行限制。

- **连接数限制**：控制指定用户对外发起或接收的会话连接数；
- **带宽限制**：控制指定用户上传报文流量和下载报文流量带宽。






- 限流策略功能包括：
  - IP连接数限制：对指定IP发起的连接数量或接收的连接数量进行限制；
  - IP带宽限制：对指定IP的会话带宽进行限制。
- 连接数限制能达到控制用户对外发起攻击、保证其他正常业务的转发，带宽限制能起到均化网络流量、保证用户的正常访问速率、辅助防范网络攻击的作用；
- 防火墙上的带宽和连接数限制均有八个级别，用户可在指定范围内配置连接数/带宽限制等级，结合ACL限制连接数/带宽。

# 二级限流策略



**每IP限流策略（一级限流）**

- 每IP限流策略，是针对每个IP（源IP或者目的IP）单独进行限制的，其中策略约束条件包括五元组、时间段、用户身份以及应用协议。



**整体限流策略（二级限流）**

- 整体限流是针对一个域间关系上或者某个域内所有数据流进行整体管控，其中策略约束条件包括五元组、时间段、用户身份，应用协议。

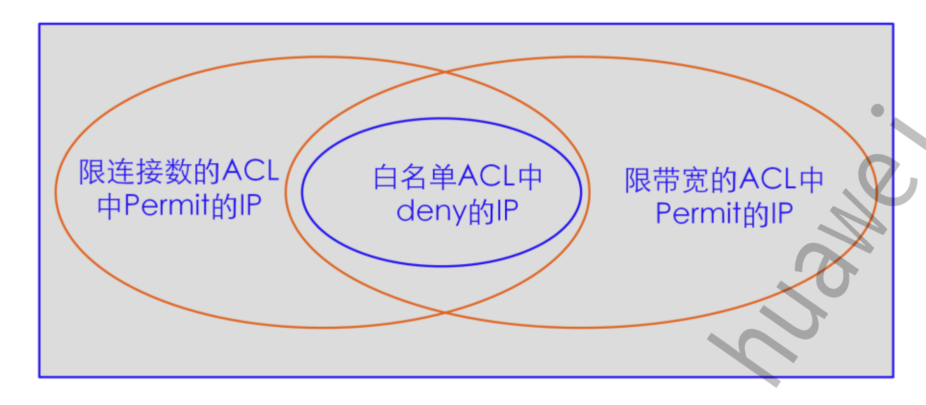




HUAWEI

- 每IP限流策略（一级限流）
  - 最大带宽：对单个IP的数据流进行最大带宽限制。
  - 保证带宽：对单个IP的数据流进行保证带宽限制。
  - 最大连接数：对单个IP的数据流进行最大连接数限制。
- 整体限流策略（二级限流）
  - 最大带宽：对整个域间或域内的数据流进行最大带宽限制。
  - 最大连接数：对整个域间或域内的数据流进行最大连接数限制。

## 白名单ACL对限流策略的影响

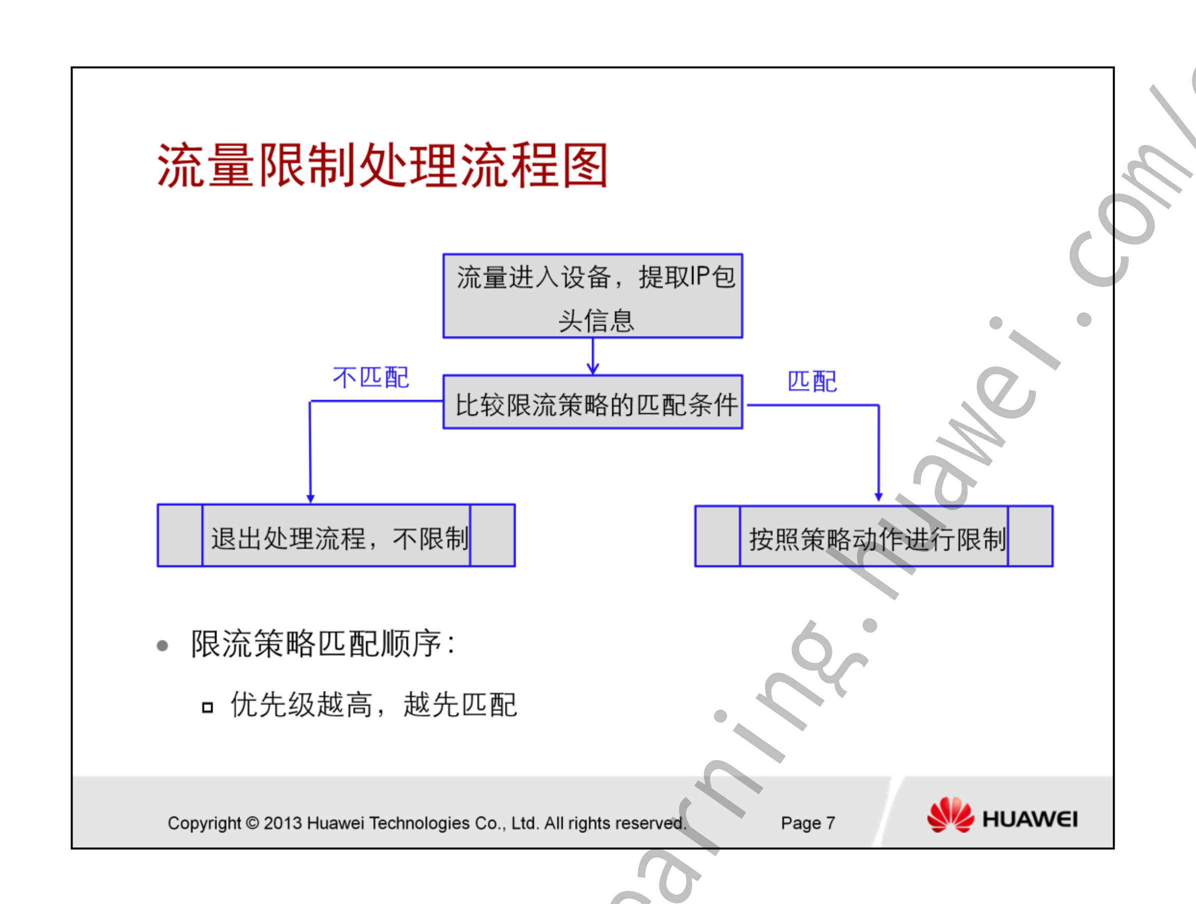



- 限连接数IP地址范围；
- 限带宽IP地址范围；
- 即受连接数限制又受带宽限制IP地址范围。

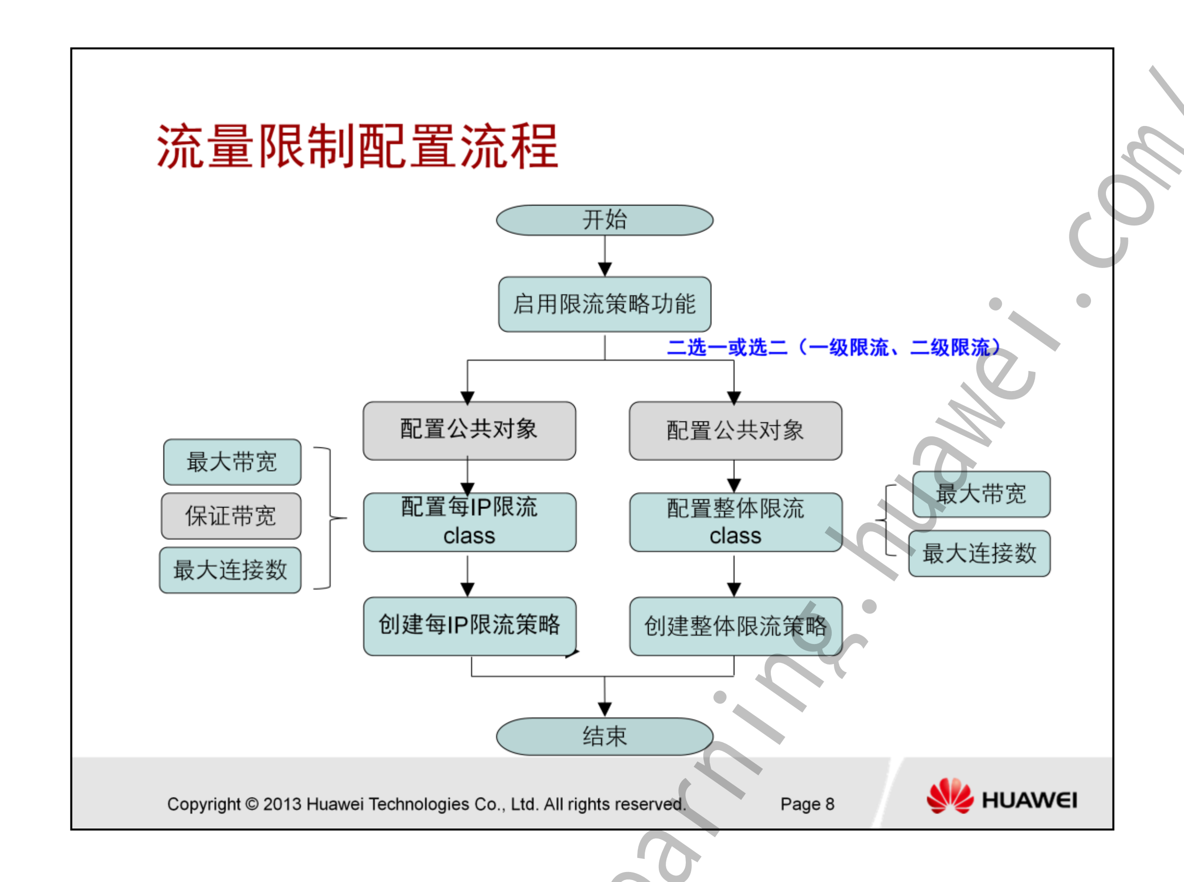




- 根据限流策略的处理流程，在流量限制功能中可以引用以下几种ACL来匹配流量:
  - 用来限制连接数的ACL:该ACL规定的地址范围中，动作为permit的IP会被限制连接数，动作为deny的IP不受影响;
  - 用来限制带宽的ACL:该ACL规定的地址范围中，动作为permit的IP会被限制带宽，动作为deny的IP不受影响;
  - 白名单ACL:白名单ACL中定义为deny的IP不会受到限流，所以即使在上述两条ACL中，包含了该ACL规定的地址范围且动作是permit，这些地址也不会受到限流策略功能的影响。在白名单中定义为permit的IP继续进入上述两条ACL的检查流程。
- 所以通常在创建ACL时，可以将用来限制连接数和带宽的ACL的地址范围定义得比较大，再通过白名单中deny的IP使一小部分IP不受到限流策略的影响。




域间可以应用多条限流策略，按照策略列表的顺序从上到下匹配。只要匹配到一条策略就不再继续匹配剩下的策略。缺省情况下，策略列表按策略的配置顺序排列，越先配置的优先级越高、越先匹配，但是也可以手工调整策略之间的优先级。




- 限流策略的配置流程如图所示，可根据实际场景配置（一级限流、二级限流），或者二者都配置，来对流量进行控制。
- 配置公共对象包括的内容：
  - 配置地址集
  - 配置时间段
  - 配置服务集（端口）
  - 配置应用协议集
  - 配置用户
- 限流策略与公共对象的关系如下：
  - 一个公共对象可以被多个限流策略引用。
  - 一个限流策略中可以引用多个公共对象，流量只要匹配其中一个对象就会命中限流策略。

# 配置每IP限流

- 启用限流策略功能

**traffic-policy enable**

- 进入每IP car-class视图

**car-class** *car-class-name* **type per-ip** [ **vpn-instance** *vpn-instance name* ]

- 配置每IP类型的car-class，配置限流的阈值
  - 配置最大带宽和保证带宽，保证带宽不大于最大带宽。二者值范围都8～10000000，单位：kbps。

**car** { **max** *max-value* | **guaranteed** *guaranteed-value* }

  - 配置最大连接数。取值范围是1～1000000。

**connection-number** *connection-number*








- 保证带宽是每个IP(用户)最少能获得的带宽，然后整体网络中的所有IP（用户）再通过抢占的方式，分配整体剩下的带宽。
- 保证带宽需要与整体限流结合起来使用，因为对于单个IP而言，若不配置其所在网络的整体限流，单个IP的最大带宽就相当于保证带宽，此时配置保证带宽没有意义。所以，当需要应用保证带宽功能时，必须同时配置每IP限流和配置整体限流。
- 每IP保证带宽、每IP最大带宽、整体带宽3个参数之间的关系如下：
  - 必须保证每IP的保证带宽的总值要小于整体带宽的值，这个需要先根据网络规划计算保证，保证带宽的总和不超过接口的总带宽，如果所有的流量加起来超过了运营商给的带宽，就会在接口处随机丢包。
  - 一般情况下配置保证带宽的时候只配置每IP保证带宽、整体带宽就行了，如果还需要限制每个IP的最大带宽还可以配置每IP最大带宽。此时所有IP的最大带宽的和要大于整体带宽，否则保证带宽无意义。
  - 整体限流策略和每IP限流策略控制的IP范围需一致，因为如果二者不一致，当整体带宽较小时，没有配置保证带宽的IP会因为无法抢占配置了保证带宽的IP的流量，而导致允许通过流量的很少。

当需要对某个网段实现整体限流，又要实现对其中一部分网段实现应用协议（例如：P2P等协议）的整体限流，这时，需要结合QOS等其他特性功能来实现对应用协议的限流。当配置了NAT、SLB等涉及地址转换的功能特性时，需要针对真实的IP地址进行限流配置。

# 配置每IP限流

- 根据需要选择如下命令进入域间或域内每IP限流策略视图。
  - 进入根防火墙或虚拟防火墙内部的域间每IP限流策略视图

**traffic-policy interzone** [ **vpn-instance** *vpn-instance-name*] *zone-name1 zone-name2* { **outbound** | **inbound** } **per-ip**

  - 进入跨根防火墙和虚拟防火墙的域间每IP限流策略视图

**traffic-policy interzone** *zone-name1* **vpn-instance** *vpn-instance-name* zone-name2 { **outbound** | **inbound** } **per-ip**

  - 进入根防火墙或虚拟防火墙内部的域内每IP限流策略视图

**traffic-policy zone** [ **vpn-instance** *vpn-instance-name*] *zone-name* **per-ip**






由于虚拟防火墙的所有安全域的级别都比根防火墙的高，这里Inbound表示从根防火墙到虚拟防火墙的域间，Outbound表示从虚拟防火墙到根防火墙的域间。

# 配置每IP限流

- 创建限流策略，并进入限流策略的配置视图。

**policy** [ *policy-id* ]

  - 同一个策略视图下可以为不同的流量创建不同的策略。缺省情况下，越先配置的策略，优先级越高，越先匹配报文。
  - 各个policy之间的优先级关系可以通过命令进行调整

- （可选）配置限流策略的CAR类型为针对源IP或者目的IP进行每IP限流

**policy car-type** { **source-ip** | **destination-ip** }

  - 缺省情况下，针对源IP进行限流。

- 配置每IP限流策略引用car-class

**policy car-class** *car-class-name*






每IP限流策略只能引用每IP类型的car-class，不能引用整体类型的car-class。

## 配置每IP限流

- （可选）指定需匹配流量的源地址。

**policy source** { *source-address* { *source-wildcard* | **0** | **mask** { *mask-address* | *mask-len* } } | **address-set** { *address-set-name* } <1-256> | **range** *begin-address end-address* | **any** }

- （可选）指定需匹配流量的目的地址

**policy destination** { *destination-address* { *destination-wildcard* | **0** | **mask** { *mask-address* | *mask-len* } } | **address-set** { *address-set-name* } <1-256> | **range** *begin-address end-address* | **any** }

- （可选）配置策略生效的时间段

**policy time-range** *time-name*

- （可选）指定需匹配流量的服务类型

**policy service service-set** { *service-set-name* } <1-256>






策略的服务集可以是自定义服务集也可以是预定义服务集。自定义服务集是通过命令ip service-set配置的，预定义服务集是系统预先定义的。

# 配置每IP限流

- （可选）配置策略匹配的应用协议类型。

  **policy** { **app-set** *app-set-name* | **category** *category-name* [ **application** *application-name* ] }

- （可选）指定匹配流量的用户身份，可以是发送或接收流量的用户。

  **policy** { **user** *user-name* | **user-group** *user-group-name* }

- 配置对匹配流量的采动作

  **action** { *car* | *no-car* }

- （可选）开启限流策略丢包日志发送功能

  **traffic-policy discard packet log enable**






- 配置策略匹配的应用协议类型时:
  - app-set-name表示应用协议集，应用协议集需事先通过DPI视图下的app-set命令配置方可被引用。
  - category-name表示应用协议大类，application-name表示应用协议小类。当配置大类为userdefine时，表示自定义应用协议大类，后面必须配置自定义应用协议小类。
  - 当配置基于应用协议识别的限流时，需要先执行命令dpi enable，开启DPI功能
- 配置策略后，需要对策略进行调整，可以在限流策略视图下启用或者禁用一条策略:
  - policy policy-id { enable | disable }
- 调整策略优先级
  - 将策略policy-id1优先级调整到策略policy-id2的前面

    policy move policy-id1 before policy-id2
  - 将策略policy-id1优先级调整到策略policy-id2的后面

    policy move policy-id1 after policy-id2

# 配置整体限流

- 启用限流策略功能

**traffic-policy enable**

- 进入整体car-class视图

**car-class** *car-class-name* **type shared** [ **vpn-instance** *vpn-instance name* ]

- 配置整体类型的car-class，配置基于源的整体限流的阈值
  - 配置最大带宽。取值范围是8～10000000。单位：kbps

**car** *car-value*

  - 配置最大连接数。取值范围是1～1000000。

**connection-number** *connetion-number*





# 配置整体限流

- 根据需要选择如下命令进入域间或域内每IP限流策略视图。
  - 进入根防火墙或虚拟防火墙内部的域间整体限流策略视图

**traffic-policy interzone** [ **vpn-instance** *vpn-instance-name*] *zone-name1 zone-name2* { **outbound** | **inbound** } **shared**

  - 进入跨根防火墙和虚拟防火墙的域间整体限流策略视图

**traffic-policy interzone** *zone-name1* **vpn-instance** *vpn-instance-name zone-name2* { **outbound** | **inbound** } **shared**

  - 进入根防火墙或虚拟防火墙内部的域内整体限流策略视图

**traffic-policy zone** [ **vpn-instance** *vpn-instance-name*] *zone-name* **shared**

  - 其他配置与每IP限流配置一致。






如果配置了**vpn-instance** *vpn-instance-name*参数表示进入虚拟防火墙的域间或域内整体限流策略视图。

# 检查限流策略配置

- 查看car-class的配置信息

**display car-class** { *all* | *car-class-name* | **type** { *shared* | *per-ip* } [ **vpn-instance** *vpn-instance name* ] }

- 查看所有限流策略的配置信息

**display traffic-policy all** [ **vpn-instance** *vpn-instance-name* [ **description** *description-text* ] | **description** *description-text* ]

- 查看某个域间的限流策略的配置信息

**display traffic-policy** [ **vpn-instance** *vpn-instance-name* ] *zone-name1 zone-name2* { **inbound** | **outbound** } { **share** | **per-ip** }

**display traffic-policy** *zone-name1* [ **vpn-instance** *vpn-instance-name ] zone-name2* { **inbound** | **outbound** } { **share** | **per-ip** }





# 检查限流策略配置

- 查看每IP限流策略的统计信息。

**display traffic-policy statistic per-ip** { car | connection } [ [ interzone [ vpn-instance vpn-instance-name ] zone-name1 zone-name2 { inbound | outbound } [ policy policy-id ] ] ]

- 查看整体限流策略的统计信息。

**display traffic-policy** statistic shared { car | connection } interzone [ vpn-instance vpn-instance-name ] zone-name1 zone-name2 { inbound | outbound } [ policy policy-id ]

- 清除限流策略的统计信息

**reset traffic-policy counter all**






# 查看限流策略信息

```
[USG] display traffic-policy all
  Current Total Node: 2
  traffic-policy interzone trust untrust inbound per-ip
   policy 0 (0 Times Matched)
    action car
    policy source any
    policy destination any
    policy car-type source-ip
    policy car-class class1
   policy 1 (0 Times Matched)
    action car
    policy source any
    policy destination any
    policy car-type source-ip
    policy car-class class2
```



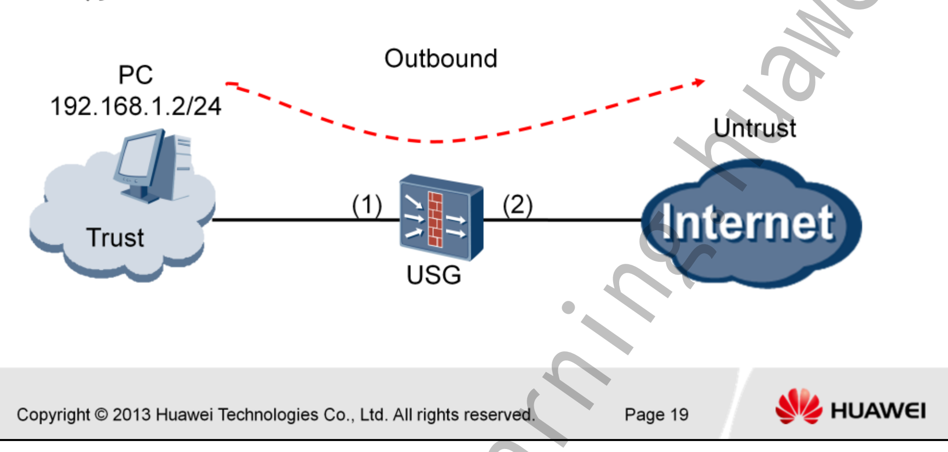





- 查看命中策略的流量统计信息

<USG> **display traffic-policy statistic per-ip car**

```
Current total node: 1
-------------------------------------------------------------------------------------------------------
IP Address        Type           SrcVrf->DstVrf          SrcZone->DstZone          PolicyID
   Passed Packets/Passed bytes     Droped Packets/Droped bytes
-------------------------------------------------------------------------------------------------------
3.4.0.15              Src               public->public                 trust->untrust            0
   1/86                    0/0
```




- 配置思路

1. 配置各个接口的IP，并加入相应的安全区域。
2. 配置域间包过滤和路由，保证网络基本通信。
3. 配置NAT功能，使内网用户能访问外网。
4. 启用限流策略功能。
5. 配置整体限流功能，限制内网用户总带宽。
6. 配置每IP限流功能，限制每个IP的保证带宽和最大带宽。

# 关键配置

- 启用限流策略功能。

  [USG] **traffic-policy enable**

- 在Trust到Untrust的inbound方向上配置整体限流策略1，引用car-class class1，限制总的下载带宽为400M。

  [USG] **car-class class1 type shared**

  [USG-shared-car-class-class1] **car 400000**

  [USG] **traffic-policy interzone trust untrust inbound shared**

  [USG-traffic-policy-interzone-trust-untrust-inbound-shared] **policy 1**

  [USG-traffic-policy-interzone-trust-untrust-inbound-shared-1] **policy car-class class1**

  [USG-traffic-policy-interzone-trust-untrust-inbound-shared-1] **policy destination 192.168.1.0 0.0.0.255**

  [USG-traffic-policy-interzone-trust-untrust-inbound-shared-1] **action car**







**policy car-class**命令用于配置限流策略引用的car-class。每IP限流策略只能引用每IP类型的car-class，不能引用整体类型的car-class；整体限流策略只能引用整体类型的car-class，不能引用每IP类型的car-class。

# 关键配置

- 在Trust到Untrust的inbound方向上配置每IP限流策略2，引用car-class class2，限制每个IP的下载保证带宽为1M，最大带宽为2M。

  [USG] **car-class class2 type per-ip**

  [USG-per-ip-car-class-class2] **car guaranteed  1000 max 2000**

  [USG] **traffic-policy interzone trust untrust 2inbound per-ip**

  [USG-traffic-policy-interzone-trust-untrust-inbound-per-ip] **policy**

  [USG-traffic-policy-interzone-trust-untrust-inbound-per-ip-2] **policy car-type destination-ip**

  [USG-traffic-policy-interzone-trust-untrust-inbound-per-ip-2] **policy destination 192.168.1.0 0.0.0.255**

  [USG-traffic-policy-interzone-trust-untrust-inbound-per-ip-2] **policy car-class class2**

  [USG-traffic-policy-interzone-trust-untrust-inbound-per-ip-2] **action car**








# 目录

1. 防火墙限流策略
2. **防火墙负载均衡**





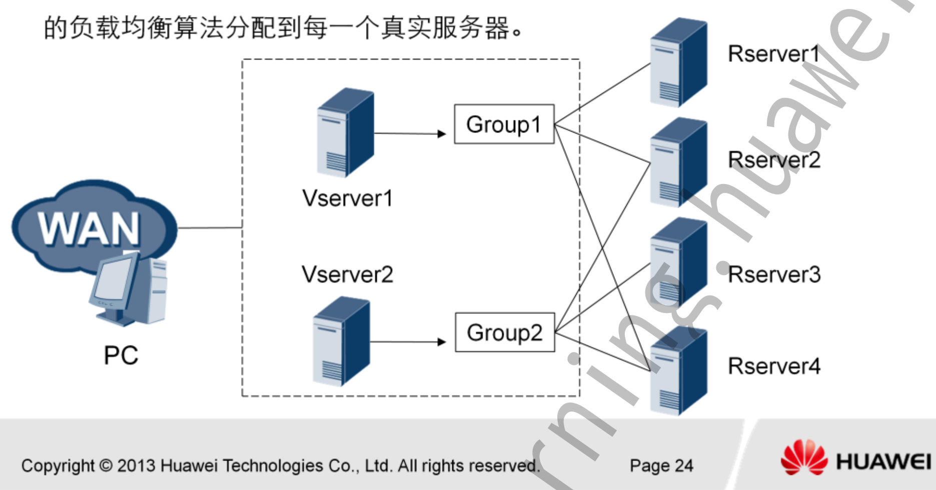

# 负载均衡概述

- 负载均衡实现了将访问同一个IP地址的用户流量分配到不同服务器上的功能。
- 负载均衡可以采用以下方法，将用户流量分配到多台服务器：
  - 虚服务技术
  - 服务器健康性检测
  - 基于流的转发






负载均衡，即设备按照配置的算法，将访问同一个IP地址的用户流量分配到不同的服务器上。在访问用户看来，他们访问的是同一个服务器，而实际上设备将他们的请求分送给了不同的服务器进行处理。这样不但可以分别利用各个服务器的处理能力，达到流量分担的目的，而且保障了服务器的可用性，得到最佳的网络扩展性。




为方便管理，在虚服务器（Vserver）和真实服务器（Rserver）之间通过服务器组Group进行衔接。Group是一个逻辑概念，USG通过Group对真实服务器进行管理，提供网络服务。

采用虚服务技术有如下优点：

- 节约公网IP地址
- 提高系统的安全性
- 提高系统的可扩展性

# 基于流的转发

- USG可以通过指定的算法，将数据流分发到各个真实服务器进行处理。
- USG支持的三种负载均衡算法:
  - 源地址哈希算法（**srchash**）
  - 简单轮询算法（**roundrobin**）
  - 加权轮询算法（**weightrr**）






服务器健康性检测是指USG向真实服务器发送健康性检测报文,周期性探测真实服务器。如果能收到真实服务器回应的报文，说明真实服务器可用；如果多次收不到服务器的回应报文，将禁止使用该真实服务器，将流量按配置好的策略分配到其他真实服务器上。

# 负载均衡配置命令（1）

- 启用负载均衡功能

**slb enable**

- 进入slb 视图，配置真实服务器

**Rserver** *rserver-id* [ **to** *end-rserver-id* ] **rip** *ip-address* [ **active** | **inactive** | **healthchk** ] [ **weight** *weight* ] [ **description** *text* ] [ **vpn-instance** *vpn-instance name* ]

- 创建并进入服务器组视图

**group** *group-name* [ **vpn-instance** *vpn-instance name* ]

- 设置负载均衡算法

**Metric** { **roundrobin** | **srchash** | **weightrr** }








对于多个真实服务器，真实服务器需处在同一网段和安全区域中。

配置**to** *end-rserver-id*时，真实服务器ID加1递增，真实服务器地址同时加1递增。如真实服务器地址不连续递增，则需一个一个配置。

配置**active**，表示不对真实服务器进行健康状态检查，强制配置真实服务器为健康状态。

配置**inactive**，表示不对真实服务器进行健康状态检查，强制配置真实服务器为不健康状态。

配置**healthchk**，表示对真实服务器进行健康状态检查。缺省情况下，配置为healthchk。

配置**weight** *weight*，表示真实服务器的权重，USG可根据服务器的权重判断数据流应该流向哪一台服务器。

# 负载均衡配置命令（2）

- 将真实服务器添加到指定服务器组

  **Addrserver** *rserver-id* [ **to** *end-rserver-id* ] [ **vpn-instance** *vpn-instance name* ]

- 配置虚拟服务器

  **vserver** *vserver-name* **vip** *ip-address* **group** *group-name* [ { **tcp** | **udp** } [ **vport** *vport-number* [ **rport** *rport-number* ] [ **vrrp** *virtual-router-id* ] ] ] [ **vpn-instance** *vpn-instance name* ]







配置虚拟服务器时，这里的*ip-address*为虚拟服务器的IP地址，配置完该项之后，用户可以通过访问该地址，达到对真实服务器流量负载均衡的目的。*group-name*对应为上文中真实服务器组。

可以通过配置**tcp**或者**udp**来限制服务器的会话协议类型；同时，可以通过配置**vport** *vport-number*和**rport** *rport-number*来严格控制真实服务器和虚服务器的访问端口。

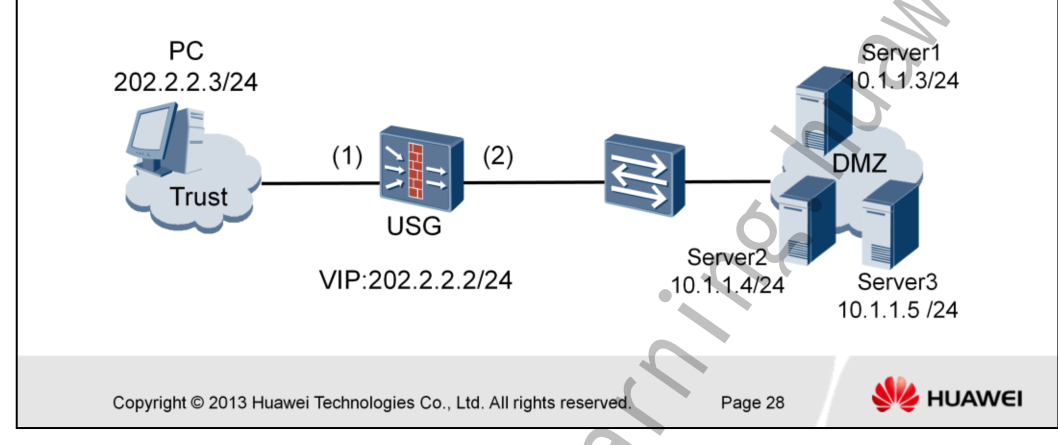
当设备同时应用于双机热备组网时，需要配置**vrrp**关键字，且*virtual-router-id*为出接口对应的VRRP备份组的ID。

配置完SLB后USG会自动对外发布虚服务器IP地址的路由信息，故无需配置与虚服务器IP地址相关的路由。

虚拟服务器IP地址不允许和真实服务器或USG接口的IP地址相同。

# 负载均衡配置举例

- 组网需求
  - 某内部网络中存在三台真实服务器对外提供FTP服务，IP地址分别为10.1.1.3/24、10.1.1.4/24和10.1.1.5/24，对外的虚拟IP地址为202.2.2.2/24。要求配置USG的负载均衡功能，保证经过USG的流量负载均衡。



# 负载均衡配置 （CLI）

1. 防火墙基础配置。（略）
2. 启用负载功能。

```
[USG] slb enable
[USG] slb
[USG-slb] rserver 1 rip 10.1.1.3 weight 32
[USG-slb] rserver 2 rip 10.1.1.4 weight 16
[USG-slb] rserver 3 rip 10.1.1.5 weight 32
```






防火墙基本配置包括：配置接口IP地址，将接口加入安全区域，配置域间包过滤规则等。

# 负载均衡配置 （CLI）

3. 配置真实服务器加入负载均衡组。

```
[USG-slb] group test
[USG-slb-group-test] metric srchash
[USG-slb-group-test] addrserver 1
[USG-slb-group-test] addrserver 2
[USG-slb-group-test] addrserver 3
```

- 说明：
  - **metric**命令用来配置负载均衡算法。其配置参数包含：
    - **Roundrobin**
    - **Srchash**
    - **weightrr**








roundrobin表示简单轮询算法：轮询选择服务器，比如第一条数据流选择第一个服务器，第二条数据流选择第二个服务器。

srchash表示源地址哈希算法：根据报文源IP地址来选择服务器，相同源IP地址数据流选择同一个服务器。

weightrr表示加权轮询算法：根据各服务器配置的权值轮询选择服务器，比如第一个服务器权值为1，第二个服务器权值为2，设备处理三个数据流时，其中一个数据流选择第一个服务器，另外两个数据流选择第二个服务器。

# 负载均衡配置 （CLI）

4. 配置虚服务器IP地址和端口号，以及真实服务器的端口号。

   [USG-slb] **vserver test vip 202.2.2.2 group test tcp vport 21 rport 21**

- 检查结果

```
<USG> display firewall session table
Current total sessions : 3
ftp VPN:public --> public 202.2.2.3:3327-->202.2.2.2:21[10.1.1.4:21]
ftp VPN:public --> public 202.2.2.3:3327-->202.2.2.2:21[10.1.1.5:21]
ftp VPN:public --> public 202.2.2.3:3327-->202.2.2.2:21[10.1.1.6:21]
```







## 负载均衡配置 （WEB）

配置负载均衡算法

配置实服务器IP地址及权值







在Web配置界面中，选择“防火墙 > NAT > 负载均衡”，选中“负载均衡功能”后面对应的“启用”复选框，单击“应用”。

选择“防火墙 > NAT > 负载均衡”，在“负载均衡列表”中，单击“新建”，依次输入或选择各项参数。

参数中，协议表示负载均衡的报文协议类型，配置此参数后对此协议的报文进行负载均衡。取值范围为any: 对任意报文均进行负载均衡； tcp: 对TCP报文进行负载均衡；udp: 对TUDP报文进行负载均衡。

算法为对流量进行负载均衡时所使用的算法。可选择roundrobin(简单轮询算法，即各个实服务器平均分配流量)，weightrr(加权轮询算法，即按照各个实服务器权值的大小分配流量，权值越大分担的流量就大，反之越小)，srchash(源地址哈希算法，即同一个源IP地址流量会分配到同一个实服务器上)。

实服务器后的权值表示真实服务器的权重设备可根据服务器的权重判断数据流应该流向哪一台服务器。处理能力弱的服务器应配置的权值较小。

连接控制表示对实服务器的连接状态进行控制。共有三种连接控制方式：

- 自动检测：对于实服务器进行自动检测连接分担流量。
- 保持连接：配置实服务器保持和网络的连接，分担流量。
- 断开连接：配置实服务器断开网络，不分担流量。



# 总结

- 防火墙限流原理与配置
- 防火墙负载均衡原理与配置






## 思考题

- 流量限制配置的思路是什么?
- 每IP限流和整体限流有什么区别?
- 什么是负载均衡?








流量限制配置的思路是什么?

答题要点：首先需要启用限流功能，然后再根据不同的流量策略选择使用整体限流还是每IP限流再进行后续配置。

每IP限流和整体限流有什么区别?

答题要点：每IP限流是根据单独的IP地址进行限流，整体限流是根据一个域间关系的数据流进行限流。

什么是负载均衡?

答题要点：负载均衡实现了将访问同一个IP地址的用户流量分配到不同服务器上的功能。




一级限流和二级限流分别表示哪种限流策略?

答案：每IP限流策略和整体限流策略



Thank you

www.huawei.com


HC120310003
防火墙可靠性技术
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



# 目标

- 学完本课程后，您将能够:
  - 掌握双机热备相关协议原理及配置
  - 掌握BFD原理及配置
  - 掌握Link-group原理和配置
  - 掌握IP-Link原理与配置
  - 掌握bypass技术原理与配置
  - 掌握Eth-Trunk原理和配置








# 目录








## IP-link基本原理介绍

- 防火墙**ip-link**功能特点
  - 检测三层链路是否可达的功能，VRRP只能探测到直连接口,三层链路探测如果探测到目的端链路不正常，能使防火墙进行主备切换，保证业务的正常；
  - 防火墙会定期向该目的地址发送icmp或ARP判断该目的地址是否可达；
  - 根据ip-link特测的结果调整VGMP的优先级实现主备切换。





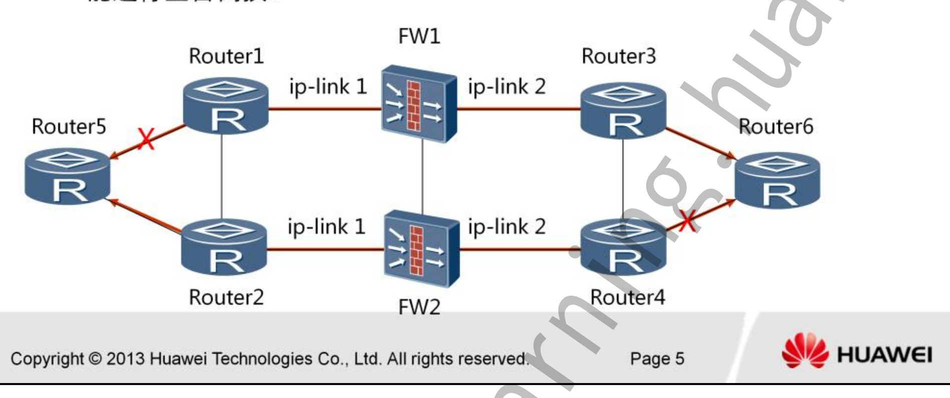

防火墙ip-link功能是一种检测三层链路是否可达的功能，基本原理就是在防火墙上配置ip-link使能并配置ip-link的目的地址之后，防火墙会向该目的地址发送icmp的报文判断该目的地址是否可达，判断从防火墙到该目的地址三层链路是否可通，应用在双机热备组网中，VGMP能根据ip-link特测的结果调整VGMP的优先级，从而使防火墙在和路由器组网中能在发生故障的时候进行主备倒换。

防火墙在使能ip-link功能时，需要判断ip-link的目的地址的设备能和防火墙进行正常的icmp交互，这样防火墙才能正确的检测该目的地址，从而在该设备发生故障的时候正确引导主备防火墙进行主备切换，所以ip-link使用的前提条件是ip-link配置的目的地址的设备能正常的和防火墙进行icmp会话。

- IP-link主要应用于：
  - 双机热备环境：当USG工作于双机热备份环境时，IP-Link自动检查后发现链路故障影响主备业务，通过配置VGMP管理组监控IP-Link，USG会对VGMP管理组的优先级进行相关调整，触发主备USG切换，从而保证业务能够持续流通。
  - 虚拟路由器冗余环境：配置VRRP监控IP-Link链路后，当IP-Link监视的链路Down时，会改变管理组的优先级，从而引起主备倒换。
  - 静态路由环境：当IP-Link自动检查发现链路故障时，USG会对自身的静态路由进行相应的调整，保证每次用到的链路是最高优先级和链路可达的，以保持业务的持续流通。
  - 策略路由环境：当IP-Link自动检查发现链路故障时，系统可以触发链路绑定的策略路由失效，这样USG在查找路由时将查找备份的路由，以保持业务的持续流通。

# IP-link功能特性

- ip-link(链路健康度检查)；
  - 组网要求当Router1和Router5之间的链路出现故障时，防火墙也需要进行主备倒换；
  - 组网要求当防火墙与Router4、Router6之间链路出现故障时，防火墙能进行主备倒换。








- 链路健康度检查的基本原理

从防火墙出发，向指定的目的地址连续发送ping报文或者arp请求报文，检查是否可以收到该目的ip应答的ping echo reply报文或arp应答报文。如果能连续3次收到，则认为该链路是稳定的；如果连续3次无法收到，则认为该链路是不稳定的。

- Ip-link探测模式（ICMP/ARP）
  - icmp模式：防火墙向需要探测的IP地址周期性发送ping报文，检查是否能连续收到对端的回应报文。Icmp探测方式可以用于探测非直连的链路；
  - arp模式：防火墙向需要探测的IP地址周期性发送arp请求报文，检查是否能连续收到对端的arp应答报文。Arp探测方式只支持探测直连链路（或中间经过二层设备转发），该探测方式不受目的IP设备上安全策略影响。

## IP-link功能配置

- 在系统视图下启动IP-Link链路检查功能

**ip-link check enable**

- 创建IP-Link链路

**ip-link** *link-id* [ **vpn-instance** *vpn-instance-name* ] **destination** { **ip-address** | **dns-address** } [ **interface** *interface-type interface-number* ] [ **timer interval** ] [ **mode** { icmp [ **next-hop** { *nexthop-address* | dhcp | dialer } ] | arp } ]

- 启用IP-Link组功能

**ip-link group enable**

- 将多个IP-Link加入IP-Link组

**ip-link group add linkid** *beginlinkID* to *endlinkID*

- 配置IP-Link组发送检测报文的时间

**ip-link group interval interval**







设备上配置数量较多的IP-Link时，这些IP-Link会同时发送链路检测报文，从而导致CPU使用率加速增长。为了解决这个问题，可以启用IP-Link组功能并将设备上的IP-Link加入IP-Link组。IP-Link组内的IP-Link会分批发送检链路测报文，从而减小设备CPU使用率的增长。

配置IP-Link组发送检测报文的时间时，interval取值越大，越能减小设备CPU的负担，但链路检测的灵敏度降低。

# IP-link功能配置

- 配置双机热备与IP-Link联动

  **hrp track ip-link** *iplink-id* { master | slave }

- 配置虚拟路由器冗余与IP-Link联动

  **vrrp** *vrid virtual-router-id* **track ip-link** *link-id*

- 配置静态路由与IP-Link联动

  **ip route-static** *ip-address* { mask | mask-length } { *nexthop-address* | **interface-type** *interface-number* [ *nexthop-address* ] } [ **preference** *preference* ] **track ip-link** *link-id* [ **description** *description* ]

- 配置策略路由与IP-Link联动
  - 配置策略路由与IP-Link联动时，没有具体命令将策略路由与IP-Link关联起来，只需将策略中设置的下一跳或缺省下一跳与IP-Link侦测的目的地址配置一致。



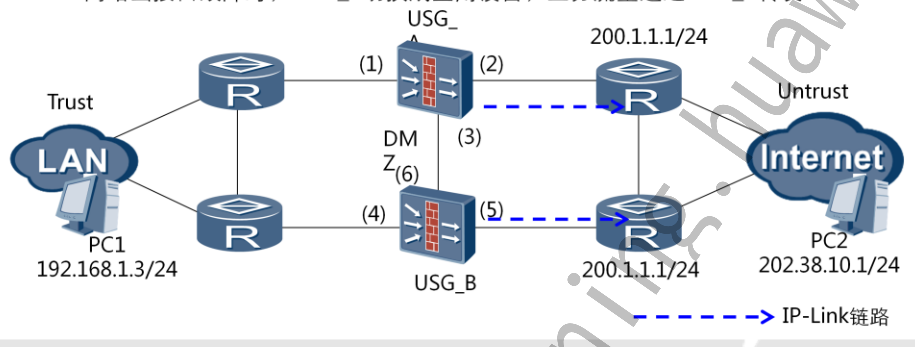




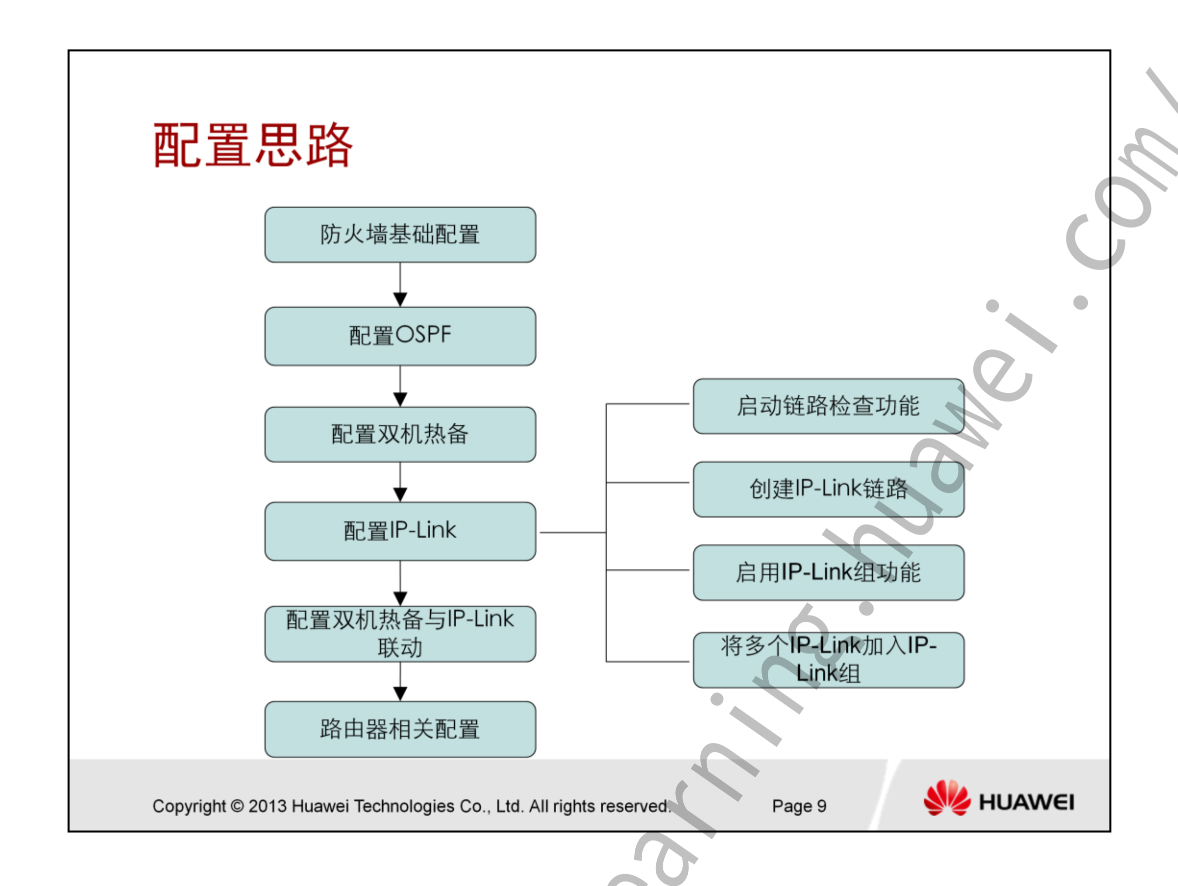
命令中参数master指定由Master管理组监视IP-Link链路状态，slave指定由Slave管理组监视IP-Link链路状态。

# 双机热备与IP-Link联动配置举例

- 组网需求
  - 配置USG的上下行业务端口加入同一Link-group管理组，在链路故障时能够加快路由收敛速度。
  - USG通过双机热备与IP-Link联动功能监控网络的出接口。当USG_A所在链路的网络出接口故障时，USG_B切换成主用设备，业务流量通过USG_B转发。






1. 在主备设备上配置USG相关接口的IP地址、将接口加入相应的安全区域，并将同一台设备的上下行接口加入同一Link-Group管理组。
2. 在主备设备上配置运行OSPF动态路由协议。
3. 在主设备接口视图下配置Master管理组监视接口状态，在备设备接口视图下配置Slave管理组监视接口状态。
4. 在主备设备上配置IP-Link功能，并通过VGMP管理组监控IP-Link。
5. 在主备设备上配置HRP备份通道，并启动HRP。
6. 在主设备上启动配置命令的自动备份、并配置Trust区域和Untrust区域的域间包过滤规则。
7. 配置路由器。

# 关键配置

- 在USG_A上配置双机热备与IP-Link联动。
  - 配置IP-Link，监控网络出接口。

    [USG_A] ip-link check enable

    [USG_A] ip-link 1 destination 200.1.1.1 interface GigabitEthernet 0/0/1
  - 配置双机热备与IP-Link联动，由VGMP管理组监控IP-Link。当网络出接口故障时，IP-Link状态变为Down，VGMP管理组优先级降低2。

    [USG_A] hrp track ip-link 1 master
- 在USG_B上配置双机热备与IP-Link联动。

  [USG_B] ip-link check enable

  [USG_B] ip-link 1 destination 202.1.1.1 interface GigabitEthernet 0/0/1

  [USG_B] hrp track ip-link 1 slave







# 目录









## BFD技术简介

- 双向转发检测BFD（Bidirectional Forwarding Detection）用于快速检测系统之间的通信故障，并在出现故障时通知上层应用。
- BFD提供两种检测模式：
  - 异步模式
  - 查询模式







BFD用于检测转发引擎之间的通信故障。具体来说，BFD对系统间的、同一路径上的一种数据协议的连通性进行检测，这条路径可以是物理链路或逻辑链路，包括隧道。

BFD的检测机制是两个系统建立BFD会话，并沿它们之间的路径周期性发送BFD控制报文，如果一方在规定的时间内没有收到BFD控制报文，则认为路径上发生了故障。

BFD控制报文封装在UDP报文中传送。会话开始阶段，双方系统通过控制报文中携带的参数（会话标识符、期望的收发报文最小时间间隔、本端BFD会话状态等）进行协商。协商成功后，以协商的报文收发时间为事件间隔在彼此之间的路径上定时发送BFD控制报文。

BFD提供两种检测模式：

异步模式：异步模式是BFD的主要操作模式。在这种模式下，BFD会话建立起来后，两个系统之间相互周期性地发送BFD控制报文，如果某个系统在检测时间内没有收到对端发来的报文，就认为此BFD会话的状态是Down。

查询模式：查询模式是BFD的第二种操作模式。当一个系统中存在大量BFD会话时，为防止周期性发送BFD控制报文的开销影响到系统的正常运行，可以采用查询模式。在查询模式下，一旦BFD会话建立，系统就不再周期性发送BFD控制报文，而是通过其他与BFD无关的机制检测连通性（比如路由协议的Hello机制、硬件检测机制等），从而减少BFD会话带来的开销。

## BFD会话状态

- BFD会话有四种状态：Down、Init、Up和AdminDown。




- 会话状态通过BFD控制报文的State字段传递，系统根据自己本地的会话状态和接收到的对端会话状态驱动状态改变。
- BFD会话的建立有两种方式，即静态配置BFD会话和动态建立BFD会话。

 Page 13 


BFD通过控制报文中的My Discriminator和Your Discriminator区分不同的会话。静态和动态创建BFD会话的主要区别在于My Discriminator和Your Discriminator的配置方式不同。

- 静态配置BFD会话

静态配置BFD会话是指通过命令行手工配置BFD会话参数，包括了配置本地标识符和远端标识符等，然后手工下发BFD会话建立请求。

- 动态建立BFD会话

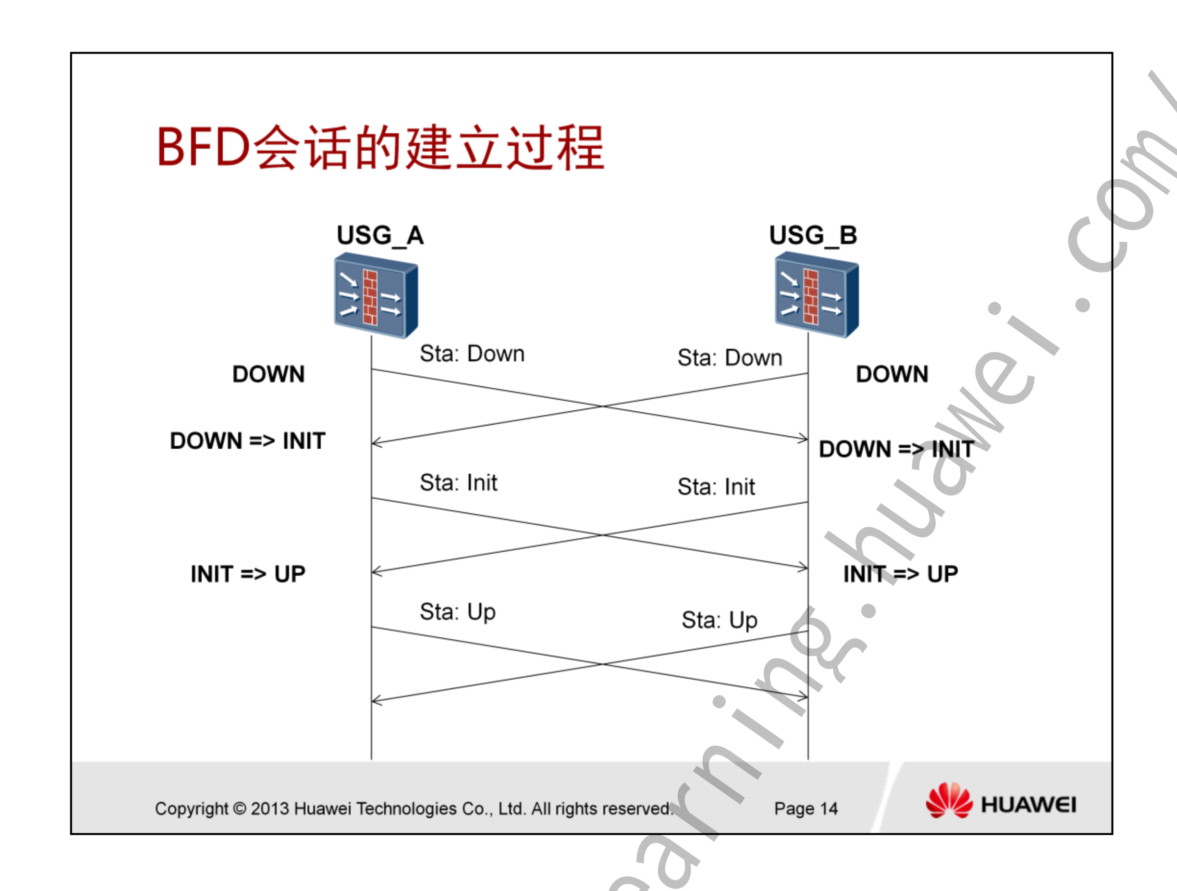
动态建立BFD会话时，系统对本地标识符和远端标识符的处理方式如下：

  - 动态分配本地标识符

当应用程序触发动态创建BFD会话时，系统分配属于动态会话标识符区域的值作为BFD会话的本地标识符。然后向对端发送Your Discriminator的值为0的BFD控制报文，进行会话协商。

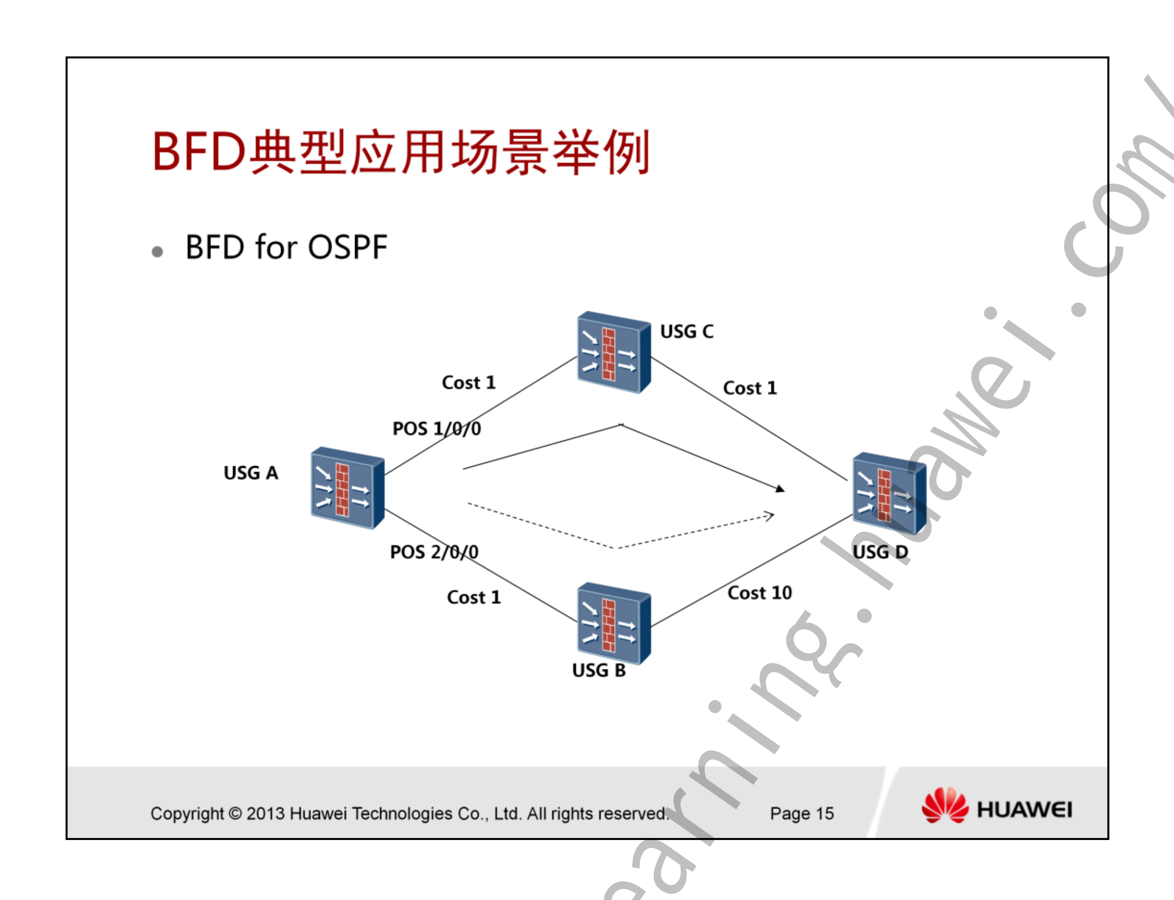
  - 自学习远端标识符

当BFD会话的一端收到Your Discriminator的值为0的BFD控制报文时，判断该报文是否与本地BFD会话匹配，如果匹配，则学习接收到的BFD报文中My Discriminator的值，获取远端标识符。




BFD状态机的建立和拆除都采用三次握手机制，以确保两端系统都能知道状态的变化。

1. USG A和USG B各自启动BFD状态机，初始状态为Down，发送状态为Down的BFD报文。对于静态配置BFD会话，报文中的Your Discriminator的值是用户指定的；对于动态创建BFD会话，Your Discriminator的值是0。
2. USG B收到状态为Down的BFD报文后，状态切换至Init，并发送状态为Init的BFD报文。
3. USG B本地BFD状态为Init后，不再处理接收到的状态为Down的报文。
4. USG A的BFD状态变化同USG B。
5. USG B收到状态为Init的BFD报文后，本地状态切换至Up。
6. USG A的BFD状态变化同USG B。
7. USG A和USG B发生“DOWN => INIT”的状态迁移后，会启动一个超时定时器。如果定时器超时仍未收到状态为Init或Up的BFD报文，则本地状态自动切换回Down。




网络上的链路故障或拓扑变化都会导致USG重新进行路由计算，要提高网络的可用性，缩短路由协议的收敛时间非常重要。由于链路故障无法完全避免，因此，加快故障感知速度并将故障快速通告给路由协议是一种可行的方案。

BFD for OSPF就是将BFD和OSPF协议关联起来，通过BFD对链路故障的快速感应进而通知OSPF协议，从而加快OSPF协议对于网络拓扑变化的响应。配置BFD for OSPF特性，可以使主链路出现故障了之后迅速切换到备份链路。

除此之外，还可以将BFD与静态路由、BGP、HRP进行绑定，用于检测链路故障。

在双机热备份组网环境下，当USG的上下行链路发生故障时，需要进行HRP主备状态的切换，以确保业务正常进行。通过配置BFD，可以快速检测到USG上下行链路的故障，也可以快速检测与USG不直接相连的链路的故障。通过配置HRP绑定BFD，在BFD会话快速检测到链路DOWN时，立即降低主用USG上VGMP管理组对应的优先级，从而触发HRP主备状态的快速切换。链路状态恢复正常时，被绑定的BFD能够检测到链路状态的变化，恢复USG上VGMP管理组的优先级。

## 关键配置命令

- BFD For OSPF的关键配置在于需要在加入OSPF域的所有防火墙上使能全局BFD特性

  [USGA] **bfd**

  [USGA] **ospf**

  [USGA-ospf-1] **bfd all-interfaces enable**

- 其次，在发送和接受BFD检测会话的接口上配置上BFD特性

  [USGA] **interface gigabitethernet 2/0/0**

  [USGA-GigabitEthernet2/0/0] **ospf bfd enable**

  [USGA-GigabitEthernet2/0/0] **ospf bfd min-tx-interval 500 min-rx-interval 500 detect-multiplier 4**








ospf bfd min-tx-interval 500 min-rx-interval 500 detect-multiplier 4命令中min-tx-interval和min-rx-interval表示指定最小发送和接收间隔为500ms，detect-multiplier表示本地检测时间倍数为4。



# 目录

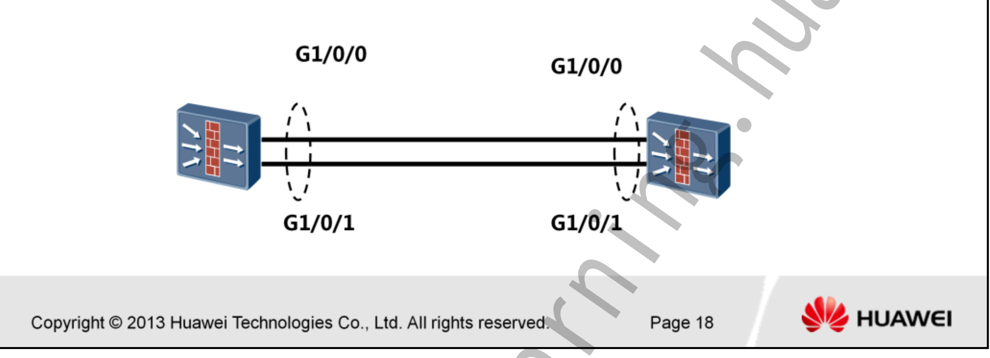
1. IP-link技术
2. BDF技术
3. **Eth-Trunk技术**
4. Link-group技术
5. Bypass技术
6. 双机热备技术






## Eth-trunk功能特性

- Eth-trunk功能是绑定多个以太网接口，形成一个逻辑接口组
- Eth-trunk功能特性如下
  - 提高链路的通讯带宽；
  - 流量的负载分担；
  - 提高链路的可靠性。






- 通过Eth-Trunk 接口可以提高链路的通信能力

　　需要将多个以太网端口捆绑为一个Eth-Trunk 接口，Eth-Trunk 接口的总带宽是各成员带宽之和，通过这种方式，可以增加接口的带宽。

- 通过Eth-Trunk 接口可以实现负载分担

　　Eth-Trunk 接口将流量分散到不同的链路上，最后到达统一目的地。这样可以避免流量都走同一条路径造成的流量阻塞。

- Eth-Trunk 接口还可以提高链路的可靠性

　　在Eth-Trunk 接口中，如果某个成员端口状态，为Down，流量还能依靠其他的端口进行传输。

- 链路聚合根据是否启用链路聚合控制协议分为以下两种类型：
  - 手工链路聚合

    　　手工模式是一种最基本的链路聚合方式，在该模式下Eth-Trunk接口的建立，成员接口的加入，以及哪些接口作为活动接口完全由手工来配置，没有链路聚合控制协议的参与。

  - 静态LACP模式链路聚合

    　　静态LACP模式下，Eth-Trunk接口的建立，成员接口的加入，都是由手工配置完成的。但与手工负载分担模式链路聚合不同的是，该模式下LACP协议报文负责活动接口的选择。

# Eth-trunk配置命令

- 创建Eth-trunk接口

  [USG]**interface eth-trunk** <*trunk-id*>

  [USG-type interfacer-number] **ip address** <*ip address*> {**mask** | **mask-lenth**}

- 物理接口加入Eth-trunk接口

  [USG]**interface** *interface-type interface–number*

  [USG-type interfacer - number]**eth-trunk** <*trunk-id*>

- 配置Eth-Trunk接口的负载分担方式

  [USG]**interface eth-trunk** <*trunk-id*>

  [USG]**load-balance** { **src-dst-ip** | **packet-all**}

- 配置负载分担权重

  [USG] **distribute-weight** *weight-value*



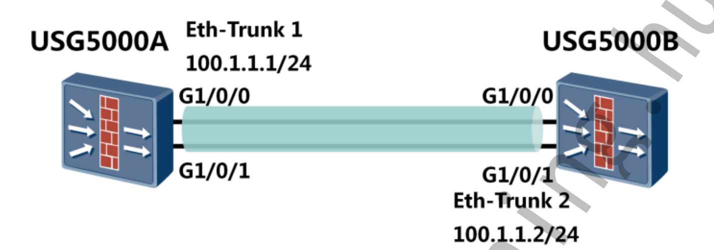




- 负载分担分为逐流负载分担和逐包负载分担。
  - 逐流负载分担是指当报文的源IP地址和目的IP 地址都相同时，这些报文从同一个的成员链路上通过。
  - 逐包负载分担是以报文为单位分别走不同的成员链路。

# Eth-trunk配置实例

- 创建eth-trunk 1组
  [USG5000A] **interface eth-trunk 1**
  [USG5000A-Eth-Trunk1] **ip address 100.1.1.1 24**
- 接口加入到eth-trunk 1组
  [USG5000A] **interface Gigabitethernet 1/0/0**
  [USG5000A- Gigabitethernet 1/0/0] **eth-trunk 1**










# 目录



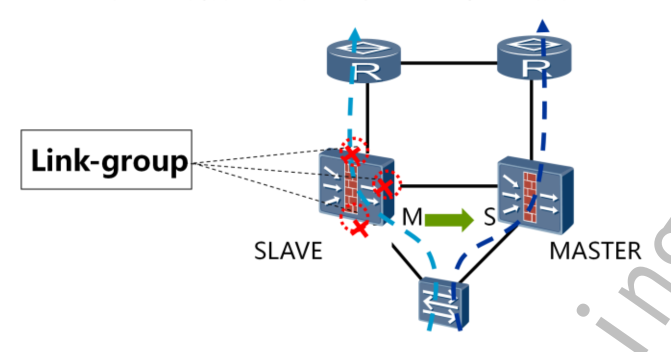






## Link-group工作原理

- **Link-group 的工作原理**
  - 将多个物理接口的状态相互绑定，组成一个逻辑组；
  - 如果组内任意接口出现故障，系统将组内其它接口状态设置为Down；
  - 当组内所有接口恢复正常后，整个组内的接口状态才重新被设置为Up。










- Link-group 具有如下特性:
  - 支持跨接口板的接口状态管理;
  - 支持接口板热插拔。
- 物理接口加入Link-group组配置命令：

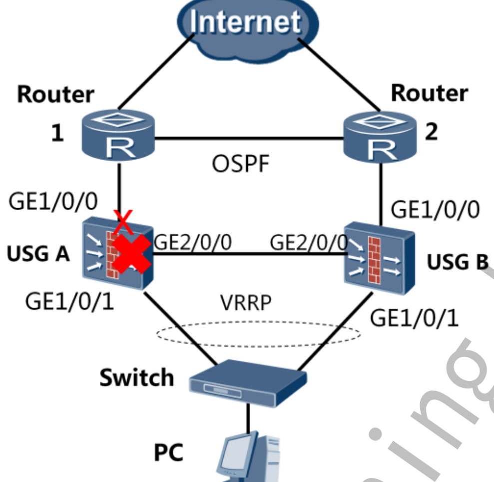
  [USG5000]system-view

  [USG5000]interface interface-type  interface-number

  [USG5000]link-group <link-group-id>

# Link-group配置实例

- 组网要求在不进行ip-link（链路检测）的情况下，当FW上行接口down，VRRP可以进行主备切换。









# Link-group实例配置

- 配置接口GigabitEthernet 1/0/0 加入到Link-group 1

  <USG> **system-view**

  [USG] **interface GigabitEthernet 1/0/0**

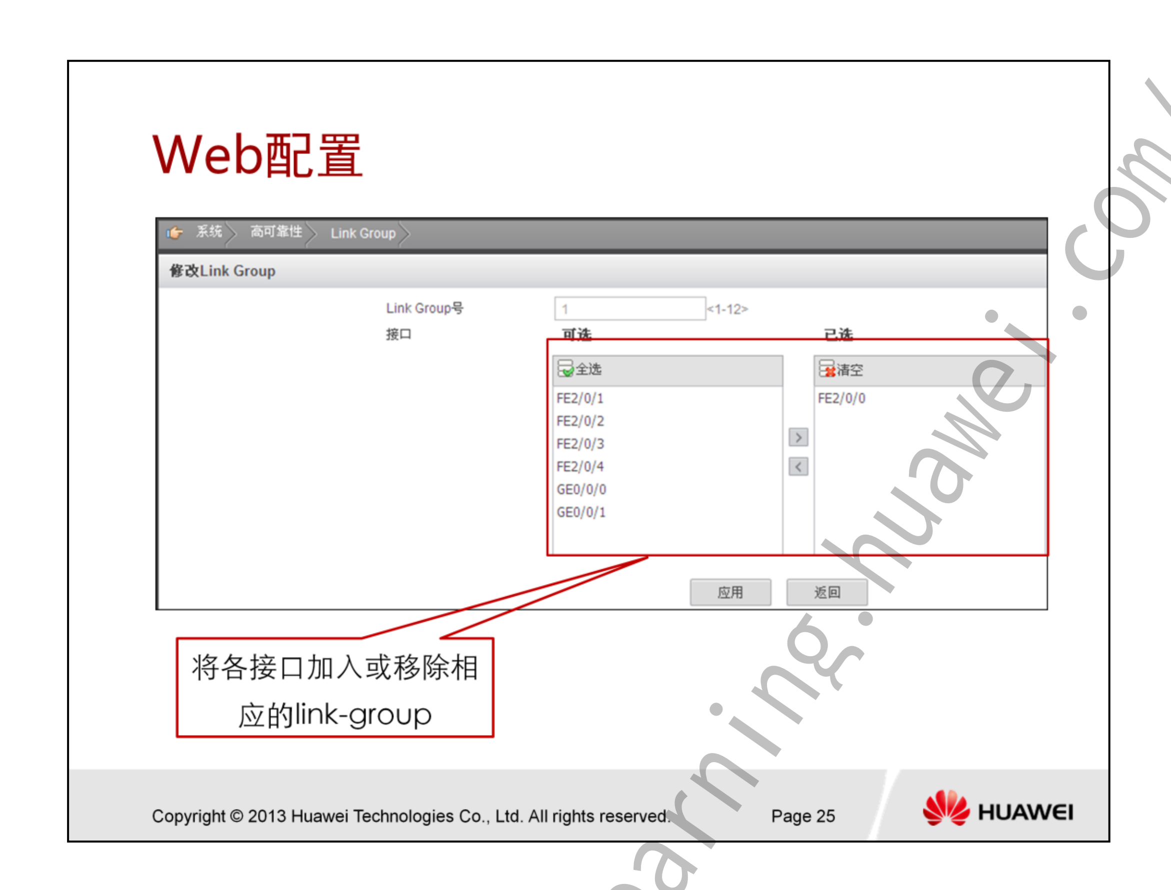
  [USG-GigabitEthernet1/0/0] **link-group 1**
- 配置接口GigabitEthernet 1/0/01加入到Link-group 1

  [USG] **interface GigabitEthernet 1/0/1**

  [USG-GigabitEthernet1/0/1] **link-group 1**






在Web配置界面中，选择系统>高可靠性>Link Group，在“Link Group”中，选择要配置的Link Group进行编辑，根据可选接口将其加入或移除Link Group。



# 目录









# 硬件Bypass技术

- 通过配置Bypass接口，可以避免设备故障引起的网络通信中断，提高网络的可靠性。Bypass功能需要Bypass接口卡的支持。
- Bypass接口分为两类：

光Bypass接口

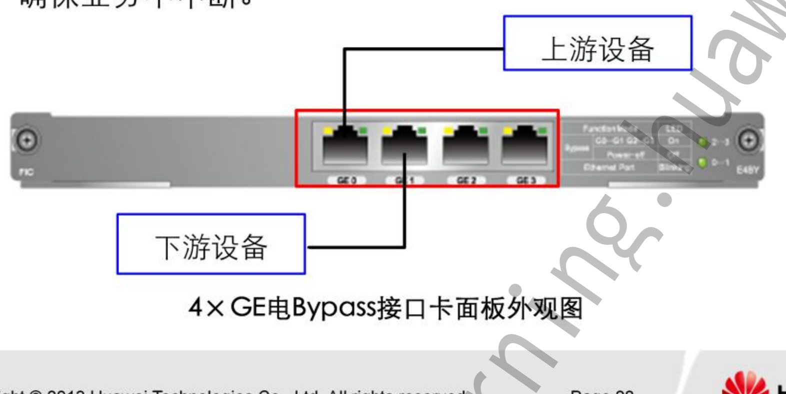
电Bypass接口





# 电Bypass接口

- 在USG防火墙上， 4×GE电Bypass接口卡对外提供4个10/100/1000M自适应以太网电接口。当USG下电或者故障时，流量可以绕过USG，使得USG两端的设备实现直接对接，确保业务不中断。




4×GE电Bypass接口卡面板外观图






4×GE电Bypass接口卡可实现数据转发功能。当4×GE电Bypass接口卡的接口工作在二层模式时，具备电路旁通功能，USG下电或者故障时，数据流可以绕过USG，使得USG两端的设备直接对接。

GE0和GE1、GE2和GE3分别组成两对Bypass接口，GE0与上游设备（Router A）连接，GE1与下游设备（Router B）连接；同理，GE2与上游设备连接，GE3与下游设备连接。

当USG正常工作时，流量由Router A从GE0接口流入USG，经过USG处理后从GE1接口流向Router B；当USG下电或者故障时，流量由Router A从GE0接口流入USG，USG不经过任何处理，直接由GE1接口流向Router B，相当于Router A与Router B直接对接。

有两种方式可以使接口处于Bypass状态:

- 自动方式。

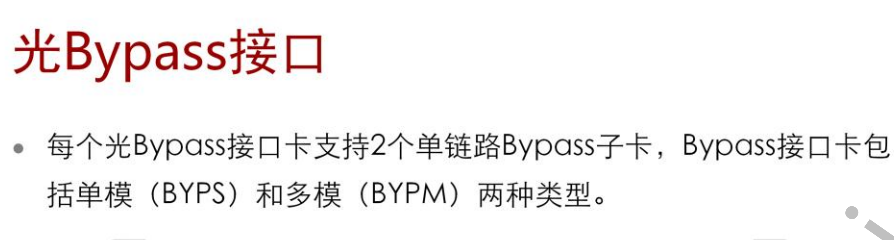
  当设备掉电的时候，支持继电器自动吸合，切换至Bypass状态。 或者当设备重启的时候，支持与主板的心跳检测，心跳丢失时切换至Bypass状态。

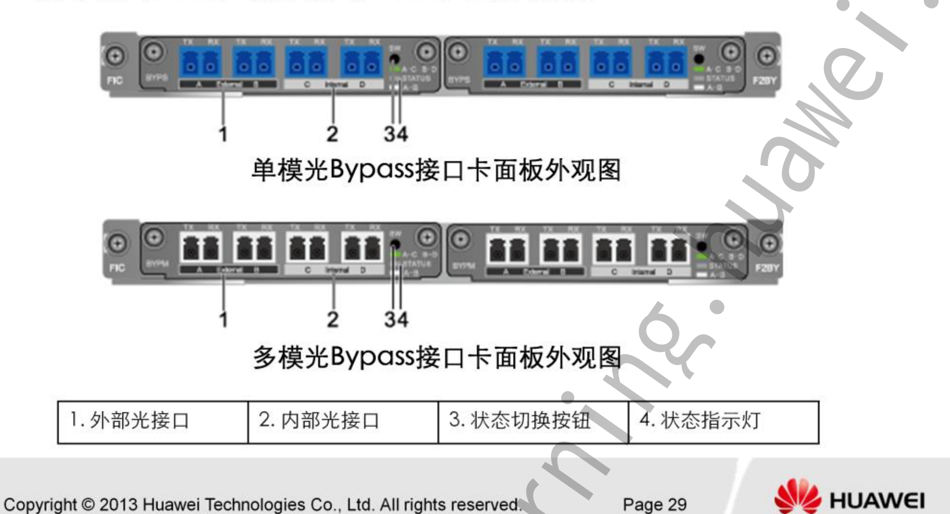
- 手动方式。

  该种方式支持手动用命令将接口切换至Bypass状态。

接口工作于Bypass状态时，业务不会中断。但是，在Bypass状态下，业务没有经过USG进行处理，存在一定的安全隐患。建议立即排除故障，并将接口恢复到非Bypass状态。

配置电Bypass接口，在系统视图下，执行命令**bypass-link** *bypass-link-number*，进入Bypass接口配置视图，然后执行命令**switch bypass**，将接口切换到Bypass状态。缺省情况下，接口处于非Bypass状态。




单模光纤芯径小（10m m左右），仅允许一个模式传输，色散小，工作在长波长（1310nm和1550nm），与光器件的耦合相对困难；多模光纤芯径大（62.5mm或50mm），允许上百个模式传输，色散大，工作在850nm或1310nm。与光器件的耦合相对容易。

Bypass链路有两种工作模式：

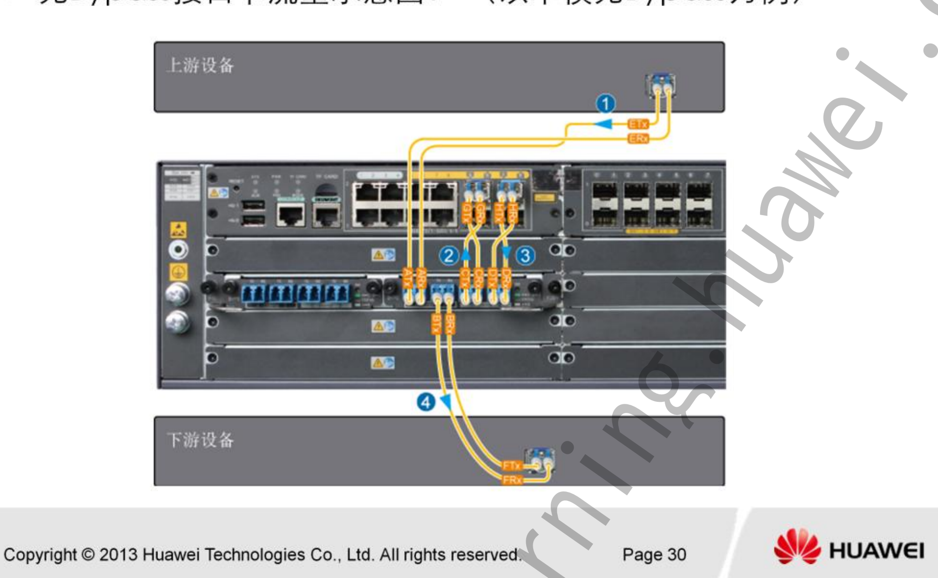
- 自动模式

如果Bypass链路处于工作回路，当Bypass链路的光功率小于工作回路LOS（Loss of signal，没有接收光信号）门限值时，Bypass链路由工作回路切换到保护回路。如果Bypass链路处于保护回路且启用自动回切功能，当Bypass链路的光功率大于工作回路LOS回滞值与LOS门限值之和时，Bypass链路在自动回切时间后由保护回路切换到工作回路。

如果Bypass链路处于工作回路，且启用了心跳功能，设备会每隔1秒向Bypass插卡（Bypass链路）发送心跳报文。如果Bypass链路在10秒内没有收到心跳报文，则由工作回路切换到保护回路。

- 强制模式

强制Bypass链路处于工作回路或保护回路，不会发生回路切换。




Bypass接口卡处于工作回路时，流量由"上游设备"经ETx流入Bypass接口卡，由Bypass接口卡C接口的CTx流入USG处理，经USG处理后再由HTx流回Bypass接口卡，最终通过Bypass接口卡B接口的BTx流入"下游设备"，流量路径为1—2—3—4。

Bypass接口卡处于保护回路时，流量由"上游设备"经ETx流入Bypass接口卡，然后直接由Bypass接口卡B接口的BTx流入"下游设备"，不经过Bypass接口卡的Internal接口和USG，流量路径为1—4。

无论Bypass接口卡处于工作回路还是保护回路状态时，Bypass接口卡均不会对流量进行任何处理。对于Bypass接口卡所在的USG来说，Bypass接口卡只是起到一个开关的作用，处于工作回路状态时，开关处于打开的状态，流量可以流入USG处理；处于保护回路状态时，开关处于关闭的状态，流量不能流入USG，直接将流量Bypass。

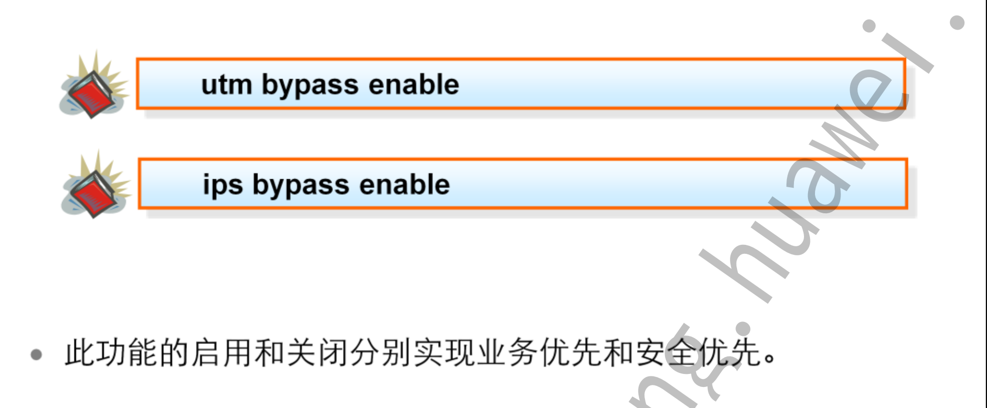
配置光Bypass接口时，执行命令**bypass-link** *bypass-link-number*，进入光Bypass链路视图。必须在与Bypass接口卡相连的光接口上配置命令**bypass enable bypass-link** *bypass-link-number*，指定Bypass链路号，确保光Bypass切换的稳定性。

其次，执行命令**mode** { **automatic** | **force** { **working-path** | **protection-path** } }，配置Bypass链路的模式和处于的回路。

缺省情况下，Bypass链路为自动模式。

# 软件Bypass命令 – 过载保护

- 启用以下两条命令可以实现设备过载保护：




- 此功能的启用和关闭分别实现业务优先和安全优先。






命令“utm bypass enable”为启用深度检测过载保护功能。启用时实现业务优先，当USG出现内存不足或者CPU处理能力达到上限的情况下，IPS、AV、升级功能自动短暂失效，报文不经过IPS、AV的检测就被转发；当USG的内存使用情况和CPU处理能力恢复正常后，IPS、AV、升级功能将自动生效。

关闭深度检测过载保护功能将实现安全优先。当USG出现内存不足或者CPU处理能力达到上限的情况下，为确保转发的报文不携带威胁，USG丢弃超过设备吞吐量的流量。

命令“ips bypass enable”为启用过载保护功能。启用时将实现业务优先，当IPS模块出现异常或IPS模块处理性能达到上限的情况下，IPS功能自动短暂失效，报文不经过IPS功能的检测就被转发，当流量恢复正常后IPS功能又自动生效。

关闭过载保护功能将实现安全优先，当IPS模块出现异常或IPS模块处理性能达到上限的情况下，为确保转发的报文不携带威胁，USG9000丢弃超过设备吞吐量的流量。

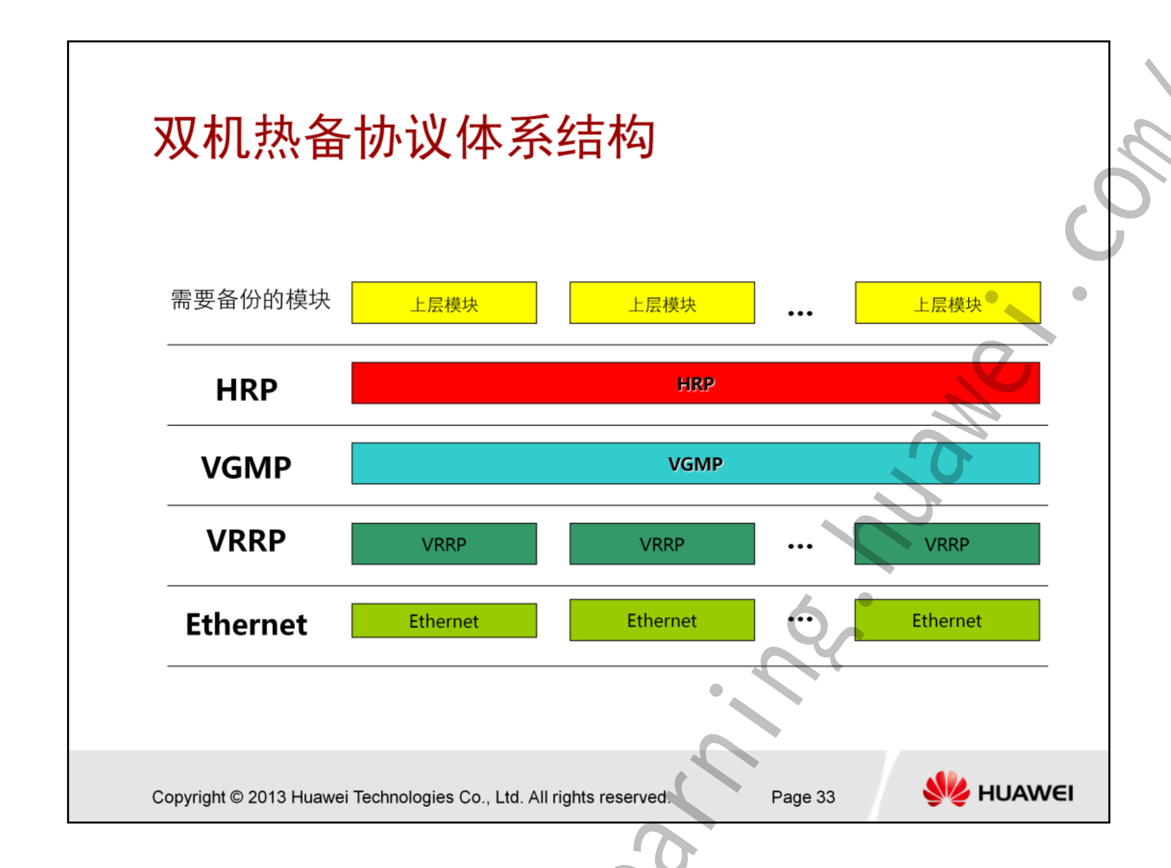


# 目录










- VRRP（Virtual Router Redundancy Protocol）是标准的协议，负责监控单个链路的状态；
- VGMP（VRRP Group Management Protocol）是对这个设备上的所有VRRP进行管理，负责监控整个设备的状态，并统一控制设备上所有VRRP备份组的状态；
- HRP（Huawei Redundancy Protocol）则负责在双机之间进行关键数据的及时同步，HRP和VGMP分工不同，之间并无功能上的联系，只是HRP报文由VGMP报文扩充而来；
- HRP只是提供了一个统一的数据同步（传输）机制，具体要发送的数据由各应用模块自己决定。




**VRRP协议原理**:

- 虚拟IP地址

同一个备份组中的多个路由器共同提供一个虚拟IP地址，作为内网用户的网关。

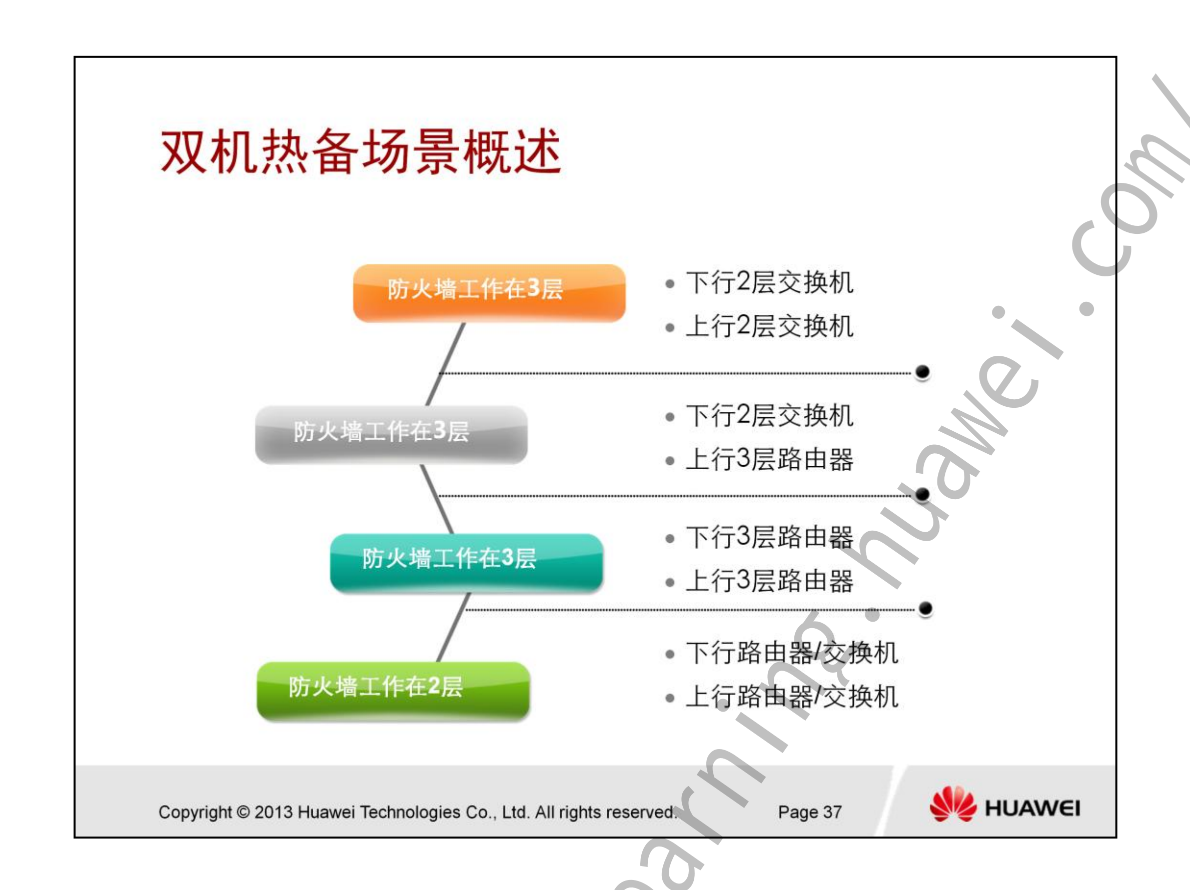
虚拟IP地址只在主路由器上生效。当主路由器故障时，会从备份路由器中选举出一个新的路由器作为主路由器，虚拟IP会自动迁移到新的主路由器。

在进行业务网关配置时，使用VRRP的虚拟IP地址来替代接口的实际IP地址，这样在出现故障时可以实现自动和平滑的切换。

- HELLO报文和故障检测

主路由器通过组播方式定期向备份路由器发送通告报文（HELLO），备份路由器则负责监听通告报文。

如果主路由器链路故障导致HELLO报文无法发送到备份路由器，当备份路由器在三个报文周期内收不到VRRP通告报文时，备份路由器就会重新协商出一个新的主路由器，该路由器将自动启用备份组的虚拟IP，同时发送虚拟IP的免费ARP报文，通知上下行设备刷新ARP表项，将业务流量切换到自己提供的业务端口，并转发以虚拟路由器IP地址作为下一跳的报文。




防火墙工作在3层模式，是指防火墙的各业务接口为三层接口需要配置IP地址。而防火墙工作在2层模式是指防火墙工作为透明模式，除HRP心跳口外，其余接口均不配置IP地址。

而防火墙工作在不同层以及其业务口所连接的设备不同，双机热备的配置也有所差异。

## HRP Track 原理

- 配置hrp track以后，接口的状态会影响对应配置的管理组的优先级。当该接口down时，所对应的管理组优先级就在原有基础上-2。
- 配置命令（在接口视图下）

**hrp track** { **master** | **slave** }

- 配置举例。在主用设备业务接口上配置hrp track如下：

[USG_A] **interface GigabitEthernet 0/0/1**

[USG_A-GigabitEthernet0/0/1] **hrp track master**

[USG_A-GigabitEthernet0/0/1] **quit**








VGMP管理组通过VRRP备份组监控接口状态。当接口或链路故障时，VRRP备份组更新自己的状态，并向VGMP管理组汇报。此外，VGMP管理组也可以直接监控上下行业务接口的状态，称为HRP Track。

每台设备的VGMP管理组初始状态由用户指定（Master或Slave），Master的优先级为65001，Slave的优先级为65000。当VGMP管理组通过VRRP备份组或直接监测到接口Down时，会重新计算VGMP管理组优先级，计算公式如下：

VGMP管理组优先级=VGMP管理组初始优先级-N*2（N=状态变为Down的被监测接口的个数）

即每个被监测的接口Down时，VGMP管理组优先级降低2。

## Vlan Track的原理和配置

- 当防火墙业务接口工作在2层时，将上行和下行业务口分别加入不同的VLAN，并在该VLAN下配置hrp track, 实现hrp track的功能。
- 配置命令（在VLAN视图下）

  **hrp track** { **master** | **slave** }
- 配置举例。在主用设备业务接口上配置hrp track如下：

  [USG_A] VLAN 2

  [USG_A- VLAN-2] **hrp track master**

  [USG_A- VLAN-2] **quit**





当USG的上下行业务接口工作在二层模式时，由于二层接口无法配置IP地址，因此无法在二层业务接口上无法配置VRRP备份组。这样就无法通过配置VRRP备份组的方式将接口加入到VGMP管理组。此时只能将上下行业务接口加入到同一VLAN，然后通过HRP Track方式由VGMP管理组监测VLAN并监测二层业务接口状态。

# 场景要点分析

- HRP Track

业务口在路由模式

- 路由器无法透传VRRP报文，通过HRP Track方式由VGMP管理组直接监测接口状态

业务口在交换模式

- 二层业务接口上无法配置VRRP备份组，通过HRP Track方式由VGMP管理组监测VLAN并监测二层业务接口状态。







## OSPF Cost调整原理

- 当防火墙上下行所连接的设备为路由器时，路由器上需要配置OSPF。而在防火墙上，需要根据HRP的状态调整OSPF Cost值，以便能主备选路。
- 配置命令（在VLAN视图下）

  **hrp ospf-cost adjust-enable** [ slave-cost ]

- 配置举例。在主用设备业务接口上配置hrp track如下：

  [USG] hrp ospf-cost adjust-enable





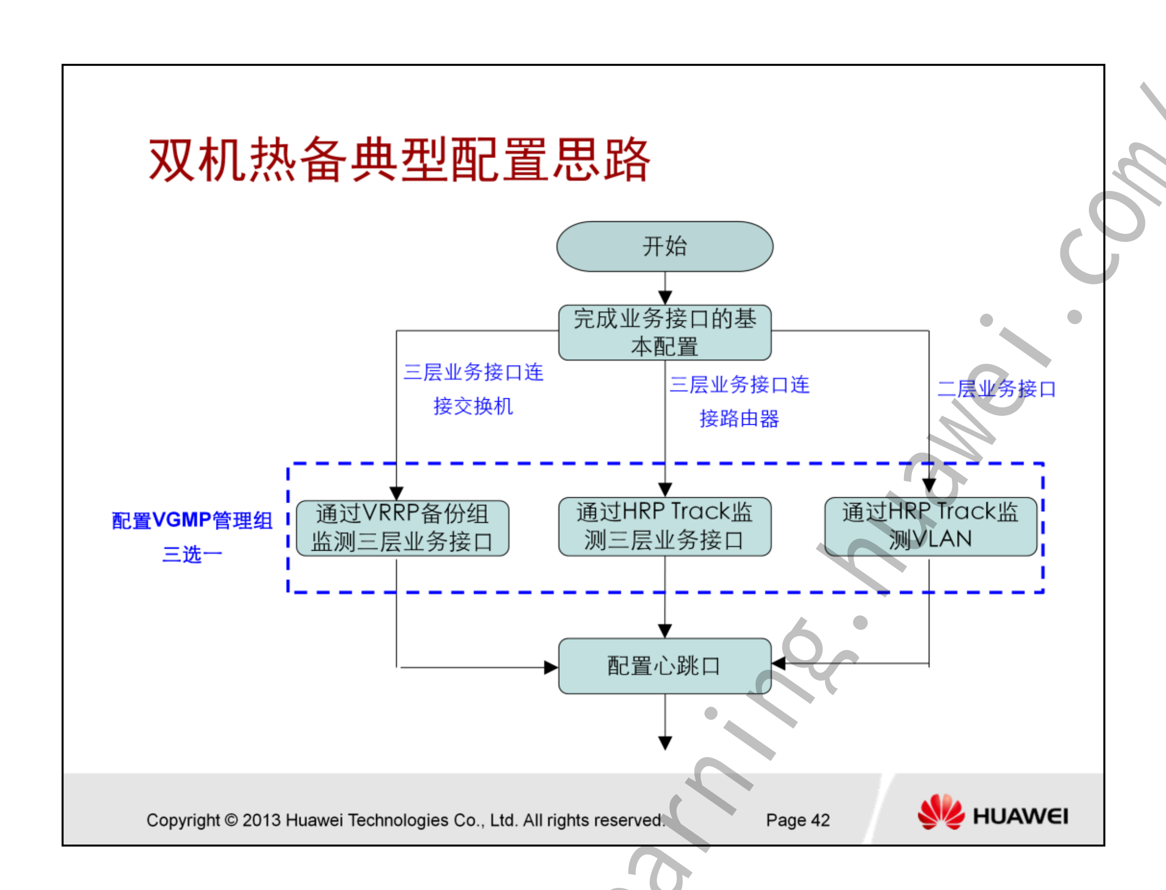

当USG部署于OSPF网络中做主备备份时，必须配置该命令。负载分担组网可以不配置此命令。

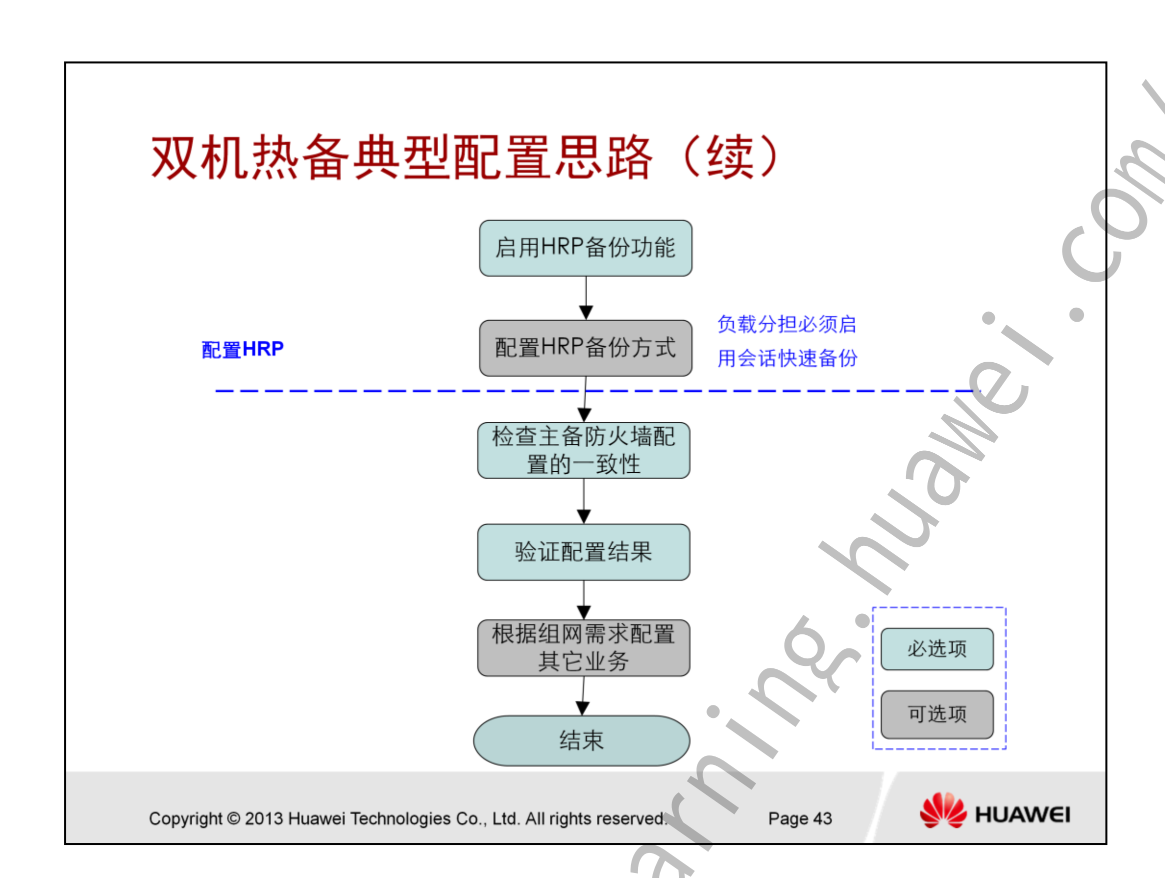
缺省情况下，此功能处于启用状态，Cost值（*slave-cost*）为65500。

*slave-cost*的取值与上下游路由器设定的OSPF Cost值有关。要求*slave-cost*的取值大于备用设备上下游路由器的Cost值。

配置这个命令后，USG发布OSPF路由时，会判断自身是主用设备还是备用设备。如果是主用设备，USG把学习到的路由直接发布出去；如果是备用设备，USG发布Cost值为*slave-cost*的路由。这样上下行路由器在计算路由的时候，就能将下一跳指向主用设备，并把报文转发到主用设备上。

当防火墙工作在2层模式且防火墙做主备备份时，并通过执行命令**ospf cost** *cost*在接口上设置OSPF Cost值。为了保证业务流量通过主用设备转发，连接主用设备的路由器的接口OSPF值需要小于连接备用设备的路由器的接口OSPF值。


双机热备典型配置思路
开始
完成业务接口的基本配置
三层业务接口连接交换机
三层业务接口连接路由器
二层业务接口
配置VGMP管理组三选一
通过VRRP备份组监测三层业务接口
通过HRP Track监测三层业务接口
通过HRP Track监测VLAN
配置心跳口
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 42
HUAWEI


双机热备典型配置思路（续）
启用HRP备份功能
配置HRP
配置HRP备份方式
负载分担必须启
用会话快速备份
检查主备防火墙配
置的一致性
验证配置结果
根据组网需求配置
其它业务
结束
必选项
可选项
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 43
HUAWEI

# 双机热备基本组网实例

- 防火墙和交换机双机热备组网，这是最成熟的双机热备组网类型
- 配置简单，倒换速度快

Master
USG_A
备份组1
Virtual IP Address
10.100.10.1/24
G0/0/0
10.100.10.2/24
G0/0/1
202.38.10.2/24
PC2:202.38.10.100/24
E2/0/0
10.0.0.1/24
Trust
Untrust
E2/0/0
10.0.0.2/24
PC1:10.100.10.100/24
G0/0/0
10.100.10.3/24
G0/0/1
202.38.10.3/24
备份组2
Virtual IP Address
202.38.10.1/24
Backup
USG_B





双机热备组网最常见的是防火墙采用路由模式，下行交换机双线上联到防火墙，正常情况下防火墙A作为主，当防火墙A上行或下行链路down掉后，防火墙B自动切换为主设备，交换机流量走向防火墙B。





防火墙双机热备基本组网主要配置命令参考：（此处仅介绍主防火墙命令行配置）

配置VRRP 备份组1和2：

[USG_A]interface GigabitEthernet 0/0/0

[USG_A-GigabitEthernet 0/0/0 ]ip address 10.100.10.2 24

[USG_A-GigabitEthernet 0/0/0 ]vrrp vrid 1 10.100.10.1 master

[USG_A]interface GigabitEthernet 0/0/1

[USG_A-GigabitEthernet 0/0/1 ]ip address 202.38.10.2 24

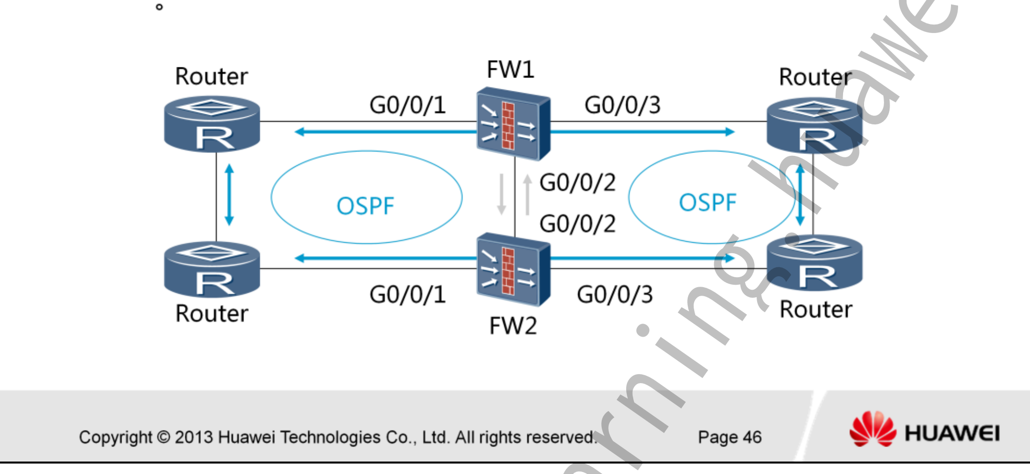
[USG_A-GigabitEthernet 0/0/1 ]vrrp vrid 1 202.38.10.1 master

配置HRP：

[USG-A]hrp enable

[USG-A]hrp mirror session enable

[USG-A]hrp interface ethernet 2/0/0





此种组网是防火墙上下行均是路由器的时候应用的最多的一种组网，对于此种组网，防火墙需要和路由器之间运行OSPF协议。

如果要形成主备组网，可以在防火墙的上下行路由器上对特定的链路调整COST值，保证业务都从同一边的路由器上转发，或者是在防火墙上配置根据HRP状态调整OSPF路由的COST值的命令，使备防火墙发布路由的时候增大COST，保证业务在同一边的路由器上转发，同时防火墙上配置一个VGMP，把所有的接口上的VRRP加入到同一个VGMP组中。

如果要形成负载分担的组网，即主备防火墙上都有转发业务，需要保证防火墙上下行的路由器上都能有业务到达防火墙，这个可以通过配置路由的方式实现。如果存在来回路径不一致的情况，需要在防火墙上配置会话快速备份功能。

- 可靠性分析：

如图所示，防火墙FW1为主防火墙，FW2为备防火墙，备防火墙向外发布路由的时候会自动加上一个COST值（默认是65500）。

- FW1和R1之间的链路故障

当FW1和R1之间的链路故障，VGMP的优先级降低，此时FW1的优先级比FW2的优先级低，防火墙发生主备倒换，FW2变成主防火墙，FW1变成备防火墙。在防火墙发生主备倒换之后，FW1和FW2都会更新自身的路由并对外发布路由，此时FW2为主，对外直接发布自身的路由，而FW1变成了备防火墙，对外发布路由的时候会另外加上一个COST值（默认是65500），路由重新计算并收敛，业务都从FW2上走。此组网图中任何一个和防火墙相连的路由器的链路down或者是路由器故障，都会引发上述过程。

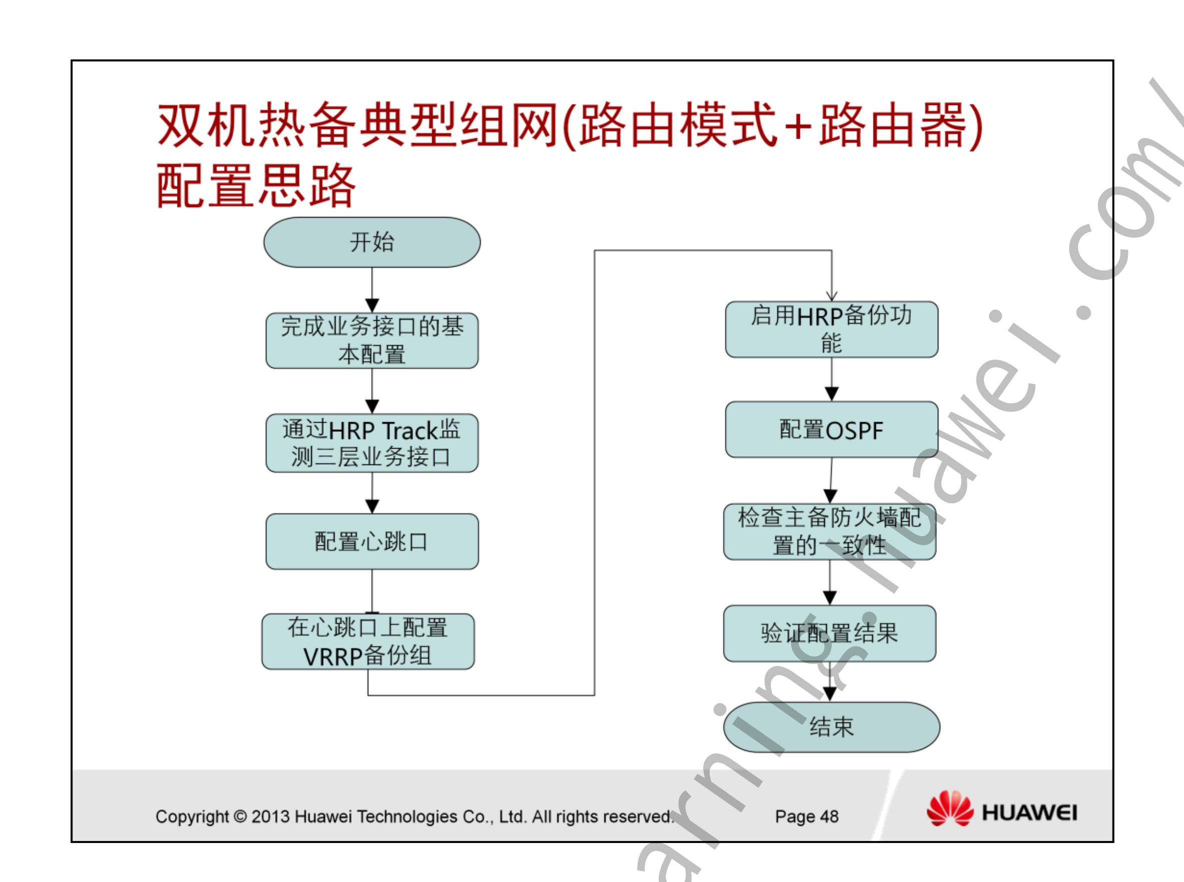



由于路由器无法透传VRRP报文，因此当USG的上下行业务接口连接路由器时，无法通过配置VRRP备份组的方式将接口加入到VGMP管理组。此时只能通过HRP Track方式由VGMP管理组直接监测接口状态。

VGMP管理组监控的接口故障时，VGMP管理组优先级降低。当主用设备的VGMP管理组优先级低于备用设备的VGMP管理组优先级，会发生主备设备的状态切换。

由于USG的上下行设备为路由器，且业务接口工作三层，因此可以在USG与上下行设备之间运行OSPF协议。如果需要实现主备备份，则需要在两台USG的直连路由器上配置不同的COST值；如果需要实现负载分担，则需要在两台USG的直连路由器上配置相同的COST值。

HRP协议可以在主用和备用设备之间实时备份关键配置命令和会话表状态信息，实现信息同步。因此需要在USG上指定心跳口，并启用HRP功能。如果是负载分担组网，为了保证流量来回路径的一致，还需要启用快速会话备份功能。


双机热备典型组网(路由模式+路由器)配置思路
开始
完成业务接口的基本配置
通过HRP Track监测三层业务接口
配置心跳口
在心跳口上配置VRRP备份组
启用HRP备份功能
配置OSPF
检查主备防火墙配置的一致性
验证配置结果
结束
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 48
HUAWEI

# 关键配置

- 在上、下行业务接口配置hrp track功能，将接口加入状态为Master的VGMP管理组。
  - [USG_A] **interface GigabitEthernet 0/0/1**
  - [USG_A-GigabitEthernet0/0/1] **hrp track master**
  - [USG_A] **interface GigabitEthernet 0/0/3**
  - [USG_A-GigabitEthernet0/0/3] **hrp track master**
- 配置根据HRP状态调整OSPF相关的COST值命令功能。
  - [USG_A] **hrp ospf-cost adjust-enable**
- 指定GigabitEthernet 0/0/2为心跳口。
  - [USG_A] **hrp interface GigabitEthernet 0/0/2**
- 启用HRP备份功能。
  - [USG_A] **hrp enable**
- 配置VGMP管理组的抢占功能为开启状态，且抢占延迟大于故障恢复后OSPF协议的收敛时间。
  - HRP_M[USG_A] **hrp preempt delay 60**







- 配置时应注意:
  - 为了保证双机备份的可靠性，建议防火墙之间采用2GE板卡，GE卡的两个口之间相连，使心跳线形成备份， 保证其中一根心跳线down掉的时候另外一根心跳线也能做备份通道;
  - 防火墙和上下行路由器起OSPF，形成动态路由，OSPF区域尽量只包含防火墙和路由器，这样路由收敛速度快，防火墙倒换过后OSPF能快速收敛。 同时不要引入心跳口IP地址的路由，保证心跳口不转发数据;
  - 需要根据HRP的状态动态调整OSPF的cost值，否则VGMP状态会是初始化状态，导致VGMP无法协商形成主备.配置VGMP为主的防火墙VGMP不抢占，避免故障恢复的防火墙在发生抢占之后路由再次需要收敛。

# 结果验证

- 检查当前HRP的状态。

```
HRP_M[USG_A] display hrp state
 The firewall's config state is: MASTER
 Current state of interfaces tracked by master:
        GigabitEthernet0/0/1 : up
        GigabitEthernet0/0/3 : up
```

- PC2作为HTTP服务器位于Untrust区域，对外提供HTTP服务。在Trust区域的PC1端访问Untrust区域的HTTP服务器，并进行文件的下载操作。分别在USG_A和USG_B上检查会话。

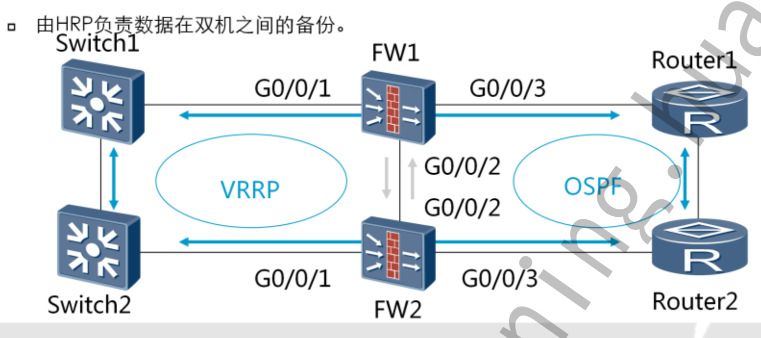
```
HRP_M[USG_A] display firewall session table
Current total sessions : 1
  http  VPN: public -> public 1.1.1.3:22048 --> 2.2.2.3:80
HRP_S[USG_B] display firewall session table
Current total sessions : 1
  http  VPN: public -> public Remote  1.1.1.3:22048 --> 2.2.2.3:80
```






# 双机热备典型组网(路由模式+上路由器下交换机)

- 组网概述：
  - 故障检测:将连接交换机接口VRRP备份组添加到VGMP管理组，由VGMP来检测防火墙下行接口运行状态；USG的上行业务接口连接路由器，通过HRP Track方式由VGMP管理组直接监测接口状态;
  - 流量切换:交换机VRRP虚地址实现流量切换,路由器和防火墙运行动态路由协议，路由cost值根据HRP状态自动调整确保来回报文从主防火墙通过；
  - 由HRP负责数据在双机之间的备份。







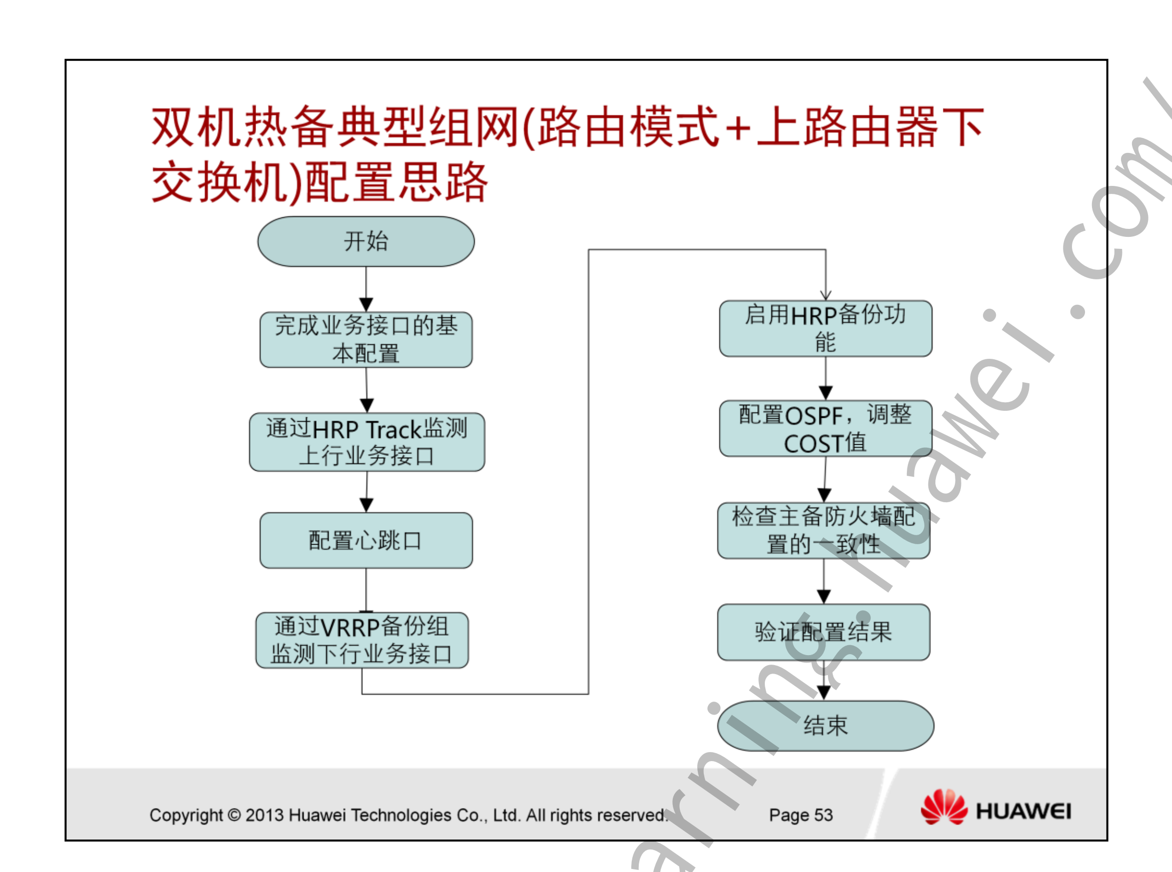

# 双机热备典型组网(路由模式+上路由器下交换机)场景分析

1. 防火墙上行是路由器下行是交换机，能适应绝大部分的组网需要
2. 通过VRRP和OSPF实现流量的快速切换
3. 下行口启用VRRP并加入相应VGMP组
4. 通过配置HRP Track方式，将上行接口加入到VGMP管理组中，监测上行业务接口状态
5. 防火墙心跳口的选择；
6. 需根据HRP状态调整OSPF COST；
7. 会话快速备份





- 配置时应注意：
  - 防火墙业务口和心跳口都采用1GE板卡，交换机相连的接口上起VRRP并加入VGMP组，同时通过HRP TRACK路由器的上行口；
  - 防火墙和上行路由器起OSPF，形成动态路由，OSPF区域尽量只包含在防火墙和路由器，这样路由收敛非常快速，防火墙倒换过后OSPF能很快收敛。同时不要引入心跳口的IP地址的路由，保证心跳口不转发数据；
  - 两台防火墙形成主备组网，需要在防火墙上配置根据HRP的状态调整OSPF的cost值的命令，根据HRP状态调整OSPF的cost值采用默认值65500就可以，如果由于组网特殊需要可以调整这个值；
  - 配置会话快速备份功能，保证发生故障防火墙倒换之后不影响业务。


双机热备典型组网(路由模式+上路由器下交换机)配置思路
开始
完成业务接口的基本配置
通过HRP Track监测上行业务接口
配置心跳口
通过VRRP备份组监测下行业务接口
启用HRP备份功能
配置OSPF，调整COST值
检查主备防火墙配置的一致性
验证配置结果
结束
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 53
HUAWEI

# 关键配置

- # 配置接口GigabitEthernet 0/0/1的VRRP备份组1，并加入到状态为Master的VGMP管理组:

  [USG_A] **interface GigabitEthernet 0/0/1**

  [USG_A-GigabitEthernet0/0/1] **vrrp vrid 1 virtual-ip 1.1.1.2 master**
- 在上行业务接口配置hrp track功能，将接口加入状态为Master的VGMP管理组。

  [USG_A] **interface GigabitEthernet 0/0/3**

  [USG_A-GigabitEthernet0/0/3] **hrp track master**
- 配置根据HRP状态调整OSPF相关的COST值命令功能。

  [USG_A] **hrp ospf-cost adjust-enable**
- 指定GigabitEthernet 0/0/2为心跳口。

  [USG_A] **hrp interface GigabitEthernet 0/0/2**
- 启用HRP备份功能。

  [USG_A] **hrp enable**

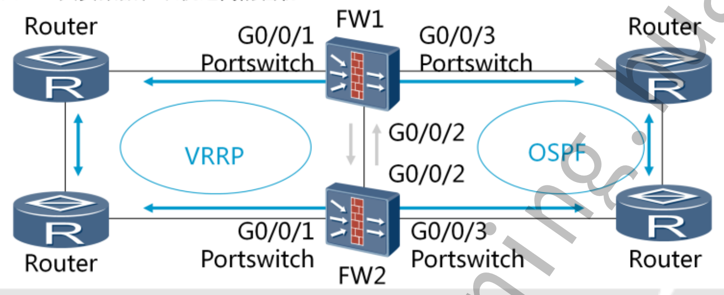






# 双机热备典型组网(交换模式+路由器/交换机)

- 组网概述：
  - 故障检测:将连接交换机接口VRRP备份组添加到VGMP管理组，由VGMP来检测防火墙下行接口运行状态；USG的上行业务接口连接路由器，通过HRP Track方式由VGMP管理组直接监测接口状态;
  - 流量切换:交换机VRRP虚地址实现流量切换,路由器和防火墙运行动态路由协议，路由cost值根据HRP状态自动调整确保来回报文从主防火墙通过；
  - 由HRP负责数据在双机之间的备份。









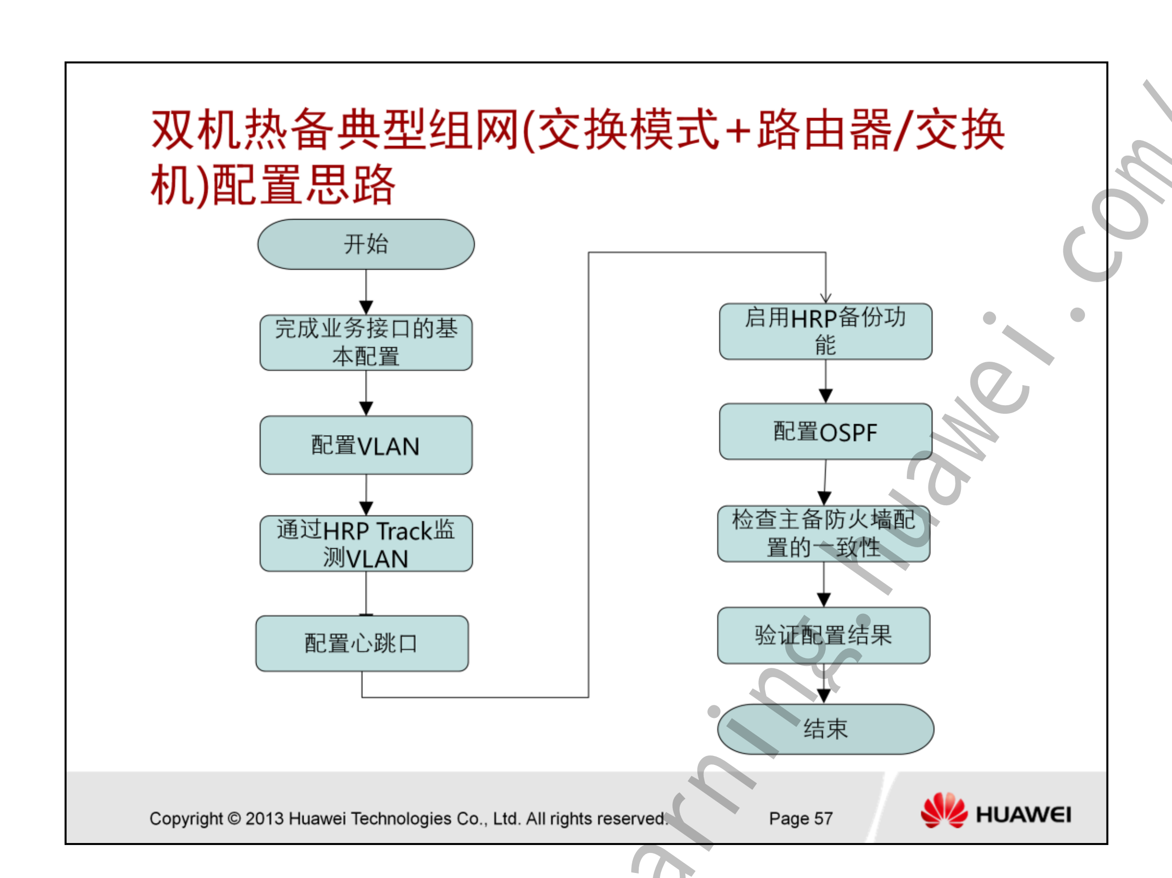



USG上、下行业务接口都工作在二层，加入同一个VLAN中，收到的所有报文都在VLAN内转发。

在VLAN下配置hrp track功能，通过VGMP管理组监控VLAN状态。当一个接口故障时，VLAN内所有接口都Down，VLAN所在的VGMP管理组优先级降低，从而实现两台USG的状态切换。

建议将上下行业务接口加入同一个Link-group组，当其中一个接口因故障而状态变为Down，将会触发组内所有接口的状态变为Down，从而保证上、下行路由器上的路由快速收敛。

启用HRP备份功能，对两台USG的状态和关键配置进行实时备份，以避免流量倒换后业务中断。


双机热备典型组网(交换模式+路由器/交换机)配置思路
开始
完成业务接口的基本配置
配置VLAN
通过HRP Track监测VLAN
配置心跳口
启用HRP备份功能
配置OSPF
检查主备防火墙配置的一致性
验证配置结果
结束
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 57
HUAWEI

# 关键配置

- 配置GigabitEthernet 0/0/1工作在二层模式。

  [USG_A] **interface GigabitEthernet 0/0/1**

  [USG_A-GigabitEthernet0/0/1] **portswitch**

- 创建VLAN，并在VLAN视图下配置hrp track功能，将接口加入到状态为Master的VGMP管理组中。

  [USG_A] **VLAN 2**

  [USG_A-VLAN-2] **hrp track master**






# 结果验证

- 在USG_A上进入VLAN视图下执行display this命令，检查VLAN 2下的配置，显示以下信息表示HRP配置成功。

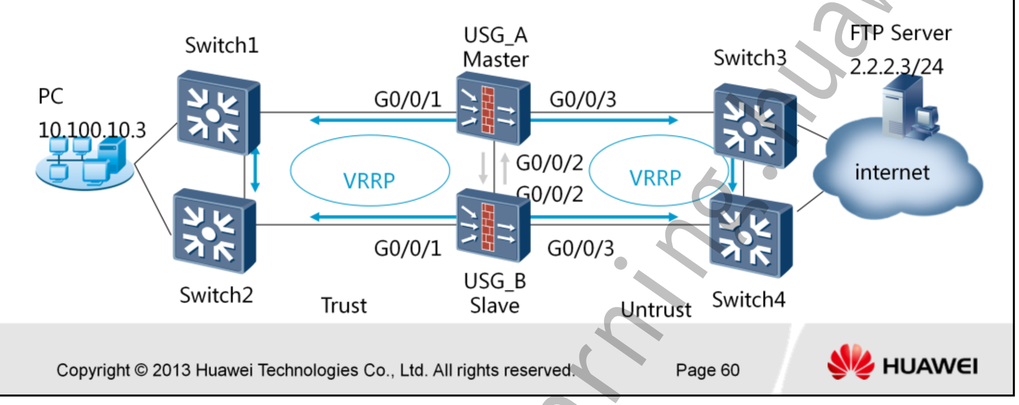
```
HRP_M[USG_A-vlan-2] display this
#
vlan 2
  hrp track master
  Tagged Ports: none
  Untagged Ports: none
#
return
```





# 双机热备与NAT结合组网

- 组网概述：
  - USG作为安全设备被部署在业务节点上。
  - 其中上下行设备均是交换机，USG_A、USG_B以主备备份方式工作，且上下行业务接口工作在三层。
  - 内网用户可以通过公网地址访问Internet，公网地址范围为2.2.2.5~2.2.2.6



# 双机热备与NAT结合组网场景分析

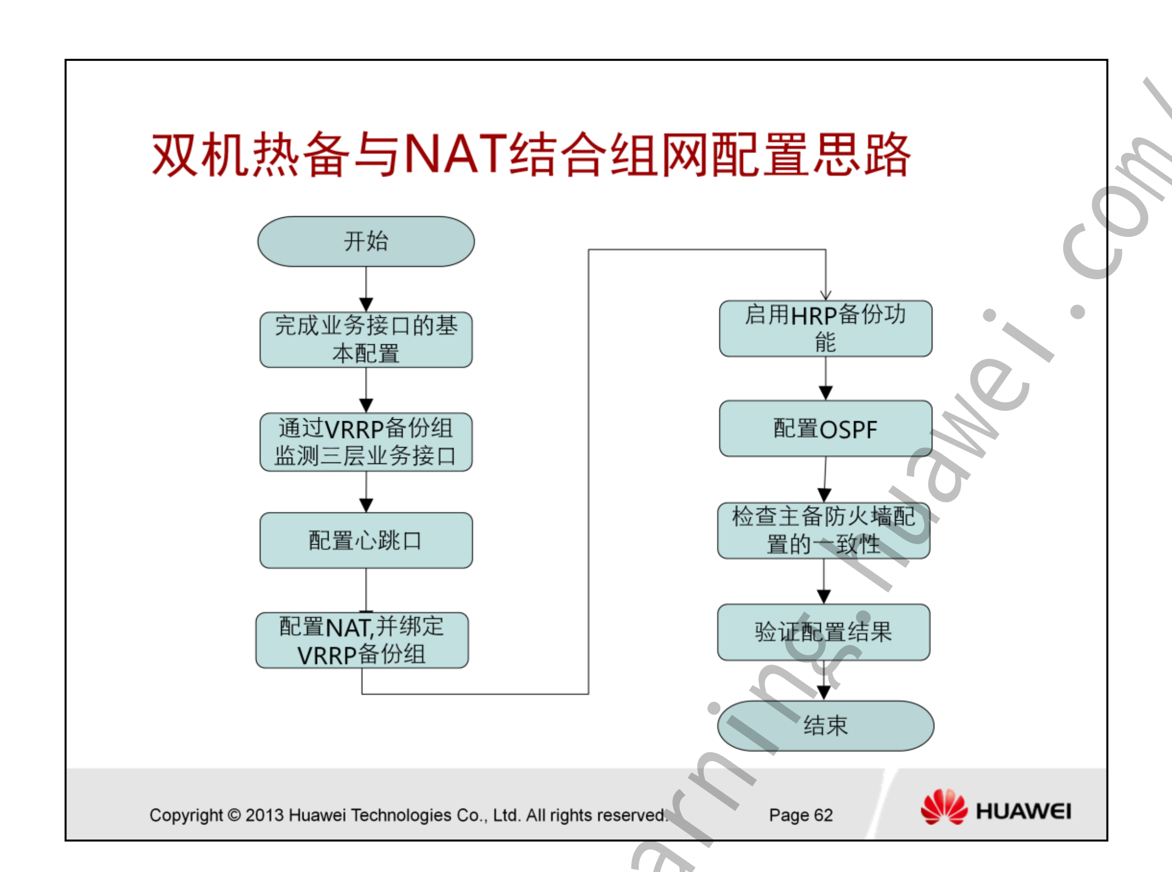
1
- 此种场景防火墙之间为双机热备并且防火墙也为NAT设备，保证内网用户能通过NAT获得公网地址访问Internet。

2
- 由于NAT地址池地址与VRRP备份组的虚拟IP地址在同一个网段，则需要将地址池绑定该VRRP备份组。

3
- 如涉及FTP等多通道协议应用，需增加NAT ALG配置。






双机热备与NAT结合组网配置思路
开始
完成业务接口的基本配置
通过VRRP备份组监测三层业务接口
配置心跳口
配置NAT,并绑定VRRP备份组
启用HRP备份功能
配置OSPF
检查主备防火墙配置的一致性
验证配置结果
结束
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 62
HUAWEI

# 双机热备与NAT结合组网关键配置

- 防火墙基本配置（略）
- 双机热备配置

  # 配置接口GigabitEthernet 0/0/1的VRRP备份组1，加入到状态为**Master**的VGMP管理组。

  [USG_A] **interface GigabitEthernet 0/0/1**

  [USG_A-GigabitEthernet0/0/1] **vrrp vrid 1 virtual-ip 10.100.10.1 master**

  # 配置接口GigabitEthernet 0/0/3的VRRP备份组2，加入到状态为**Master**的VGMP管理组。

  [USG_A] **interface GigabitEthernet 0/0/3**

  [USG_A-GigabitEthernet0/0/3] **vrrp vrid 2 virtual-ip 2.2.2.1 master**

  # 指定GigabitEthernet 0/0/2为心跳口。

  [USG_A] **hrp interface interface GigabitEthernet 0/0/2**

  #启用HRP备份功能。

  [USG_A] **hrp enable**





## 双机热备与NAT结合组网关键配置

- NAT配置

```
HRP_M[USG_A] nat address-group 1 2.2.2.5 2.2.2.6 vrrp 2
HRP_M[USG_A] nat-policy interzone trust untrust outbound
HRP_M[USG_A-nat-policy-interzone-trust-untrust-outbound] policy 1
HRP_M[USG_A-nat-policy-interzone-trust-untrust-outbound-1] policy source 10.100.10.0 0.0.0.255
HRP_M[USG_A-nat-policy-interzone-trust-untrust-outbound-1] action source-nat
HRP_M[USG_A-nat-policy-interzone-trust-untrust-outbound-1] address-group 1
```

\# 开启NAT ALG功能，保证内网用户可以与外网的FTP服务器传输数据。

```
HRP_M[USG_A] firewall interzone trust untrust
HRP_M[USG_A-interzone-trust-untrust] detect ftp
```



Page 64



当NAT地址池地址或者NAT Server的公网IP地址与VRRP组的虚拟IP地址在同一网段时，需要将地址池或者NAT Server绑定该VRRP组，防止上下行设备向NAT地址池或者NAT Server的公网IP发送ARP请求时，两台USG都会回应ARP报文，从而造成冲突，影响正常业务的运行。

在此案例中，将NAT地址池1与VRRP组2进行绑定。

# 结果验证

- 检查VRRP组内接口的状态信息

```
HRP_M[USG_A] display vrrp
 GigabitEthernet0/0/1 | Virtual Router
   1
   VRRP Group : Master
   state : Master
   Virtual IP : 10.100.10.1
   Virtual MAC : 0000-5e00-0101
   Primary IP : 10.100.10.2
   PriorityRun : 100
   PriorityConfig : 100
   MasterPriority : 100
   Advertisement Preempt : YES   Delay
    Time : 0
   Timer : 1
   Auth Type : NONE
   Check TTL : YES
```

```
GigabitEthernet0/0/3 | Virtual Router 2
   VRRP Group : Master
   state : Master
   Virtual IP : 2.2.2.1
   Virtual MAC : 0000-5e00-0102
   Primary IP : 2.2.2.2
   PriorityRun : 100
   PriorityConfig : 100
   MasterPriority : 100
   Advertisement Preempt : YES   Delay
    Time : 0
   Timer : 1
   Auth Type : NONE
   Check TTL : YES
```





# 结果验证

- 检查当前HRP的状态信息

```
HRP_M[USG_A] display hrp state
 The firewall's config state is: MASTER

 Current state of virtual routers configured as master:
           GigabitEthernet0/0/1    vrid   1 : master
           GigabitEthernet0/0/3    vrid   2 : master
```

- 查看会话表信息

```
HRP_M[USG_A] display firewall session table
Current total sessions : 2
  FTP  VPN: public -> public  10.100.10.3:2601[2.2.2.5:62691]+->2.2.2.3:21
  FTP DATA  VPN: public -> public  10.100.10.3:12288[2.2.2.5:2603]<--2.2.2.3:20

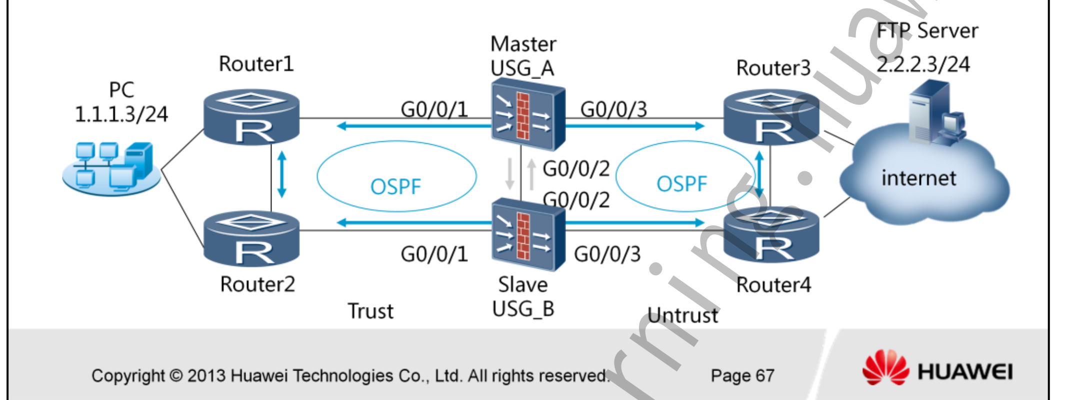
HRP_S[USG_B] display firewall session table
Current total sessions : 2
  FTP  VPN: public -> public  Remote  10.100.10.3:2601[2.2.2.5:62691]+->2.2.2.3:21
  FTP DATA  VPN: public -> public  Remote  10.100.10.3:12288[2.2.2.5:2603]<--
     2.2.2.3:20
```





# 双机热备负载分担组网（路由模式）

- 组网概述：
  - USG作为安全设备被部署在业务节点上。
  - 上下行设备均是路由器.
  - USG_A、USG_B以负载分担方式工作，业务接口工作在三层。



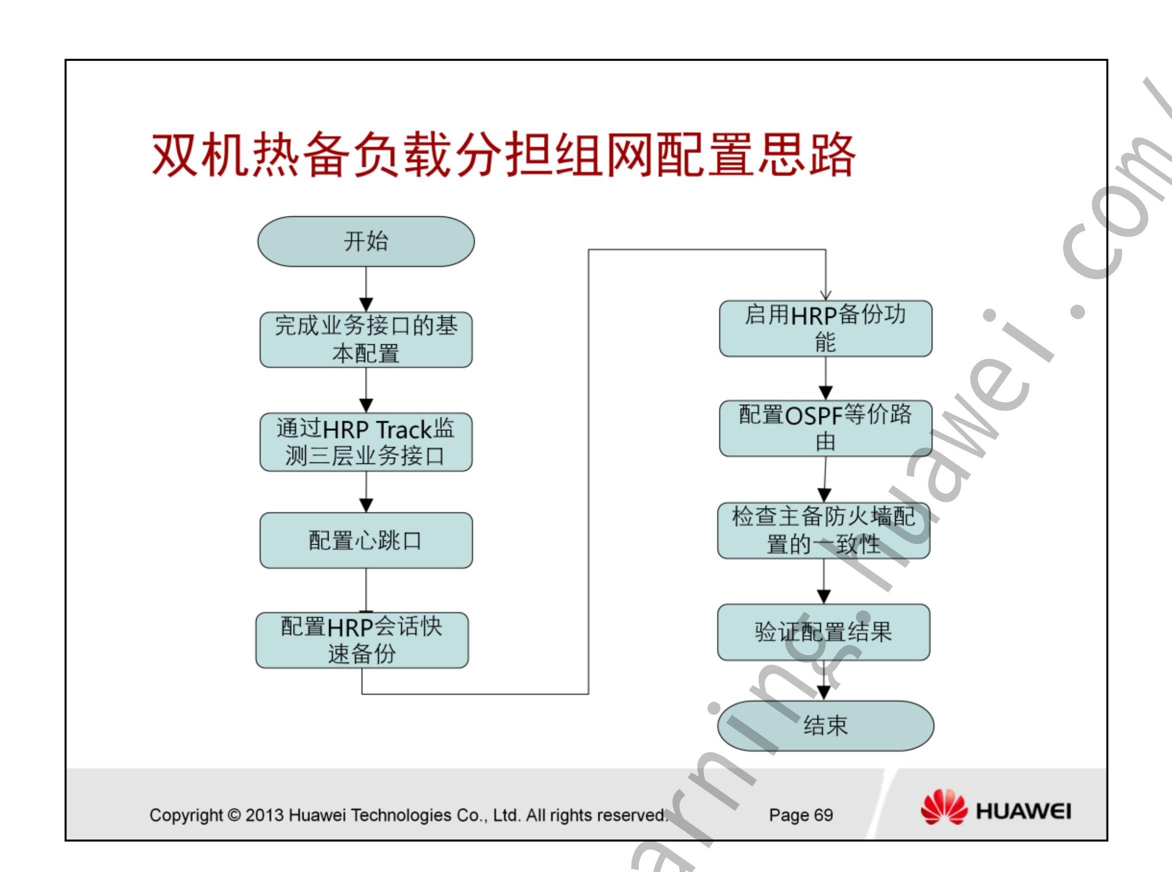
# 双机热备负载分担组网场景分析

1. 两台USG互为备份并将根据业务流情况作负载分担。
2. USG与路由器之间运行OSPF，并在上下行路由器配置等价路由，分担业务流量
3. 无需根据HRP状态调整OSPF值。
4. 配置OSPF时，为保证心跳口不转发业务报文，不将心跳口IP地址的路由引入OSPF区域。
5. 配置会话快速备份功能解决来回路径不一致的情况。



HUAWEI

1. USG上、下行业务口工作在三层，需要配置IP地址；两台USG与上、下行路由器间运行OSPF协议，通过OSPF将业务流量送到不同的USG设备上。
2. 负载分担组网时，两台USG都要转发业务流量，可以通过在上、下行路由器配置等价路由（相同的OSPF Cost值）的方式，将业务流量通过OSPF分别送到两台USG上。当其中一台USG发生故障时，OSPF可以自动收敛，将业务送到没有故障的USG上。
3. 负载分担组网时，无需配置根据HRP状态调整OSPF的COST值功能。
4. 负载分担组网中，两台USG设备互为主备，因此需要在上下行业务接口上既配置hrp track master又配置hrp track slave。
5. USG和上、下行路由器运行OSPF动态路由协议，OSPF区域尽量只包含USG和路由器，这样路由收敛速度快，USG发生主备倒换后OSPF能快速收敛。同时不要引入心跳口IP地址的路由，保证心跳口不转发业务报文。
6. 启用HRP备份功能，对两台USG的状态和关键配置进行实时备份，以避免流量倒换后，业务中断。
7. 在USG上配置会话快速备份功能，保证在来回路径不一致的情况下报文可以正常转发。


双机热备负载分担组网配置思路
开始
完成业务接口的基本配置
通过HRP Track监测三层业务接口
配置心跳口
配置HRP会话快速备份
启用HRP备份功能
配置OSPF等价路由
检查主备防火墙配置的一致性
验证配置结果
结束
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 69
HUAWEI

# 双机热备负载分担组网关键配置

- 防火墙基础配置略
- 双机热备配置(USG_A)
  - 在上、下行业务接口配置hrp track功能，将接口同时加入状态为Master和slave的VGMP管理组。

    [USG_A] **interface GigabitEthernet 0/0/1**

    [USG_A-GigabitEthernet0/0/1] **hrp track master**

    [USG_A-GigabitEthernet0/0/1] **hrp track slave**

    [USG_A] **interface GigabitEthernet 0/0/3**

    [USG_A-GigabitEthernet0/0/3] **hrp track master**

    [USG_A-GigabitEthernet0/0/3] **hrp track slave**







# 双机热备负载分担组网关键配置

- 在USG_A上配置运行OSPF动态路由协议。

  [USG_A] **ospf 101**

  [USG_A-ospf-101] **area 0**

  [USG_A-ospf-101-area-0.0.0.0] **network 10.100.10.0 0.0.0.255**

  [USG_A-ospf-101-area-0.0.0.0] **network 10.100.30.0 0.0.0.255**

- 指定GigabitEthernet 0/0/2为心跳口。

  [USG_A] **hrp interface GigabitEthernet 0/0/2**

- 启用HRP备份功能。

  [USG_A] **hrp enable**

- 启用会话快速备份功能。

  HRP_M[USG_A] **hrp mirror session enable**









# 总结

- 双机热备相关协议原理及配置
- BFD原理及配置
- Link-group原理和配置
- IP-Link原理与配置
- bypass技术原理与配置
- Eth-Trunk原理和配置







# 思考题

- 防火墙双机热备有哪几种主要场景?
- BFD是什么？有何作用?
- Link-group是什么？有何作用?
- IP-Link是什么？有何作用?
- bypass是什么？有何作用?
- Eth-Trunk是什么？有何作用?







- 防火墙双机热备有哪几种主要场景?

答题要点：根据防火墙的工作模式及上下行设备区分为不同的应用场景。

- BFD是什么？有何作用?

答题要点：BFD（Bidirectional Forwarding Detection）是双向转发检测，用于快速检测系统之间的通信故障，并在出现故障时通知上层应用。

- Link-group是什么？有何作用?

答题要点：将多个物理接口的状态相互绑定，组成一个逻辑组；如果组内任意接口出现故障，系统将组内其它接口状态设置为Down；当组内所有接口恢复正常后，整个组内的接口状态才重新被设置为Up。

- IP-Link是什么？有何作用?

答题要点：防火墙ip-link功能是一种检测三层链路是否可达的功能。可用于检测远端链路是否可达。

- bypass是什么？有何作用?

答题要点：从硬件bypass接口和软件bypass命令来分别理解。

- Eth-Trunk是什么？有何作用?

答题要点：E-trunk功能是绑定多个以太网接口，形成一个逻辑接口组。



# 练习题

- 判断题
  1. HRP技术可以实现备防火墙不需要配置任何信息，所有配置信息均由主防火墙通过HRP同步至备防火墙，且重启后配置信息不丢失。
- 单选题
  1. 以下哪个技术可实现对非直接链路状态进行检测?

  A. VGMP　B. ip-link　C. Eth-trunk　D. Link-group






习题与答案:

1. HRP技术可以实现备防火墙不需要配置任何信息，所有配置信息均由主防火墙通过HRP同步至备防火墙，且重启后配置信息不丢失。

   答案：错误

2. 以下哪个技术可实现对非直接链路状态进行检测?

   A. VGMP　B. ip-link　C. Eth-trunk　D. Link-group

   答案：B

Thank you

www.huawei.com


HC120310003
虚拟防火墙技术
www.huawei.com
Copyright ©2013 Huawei Technologies Co. ,Ltd. All rights reserved.
HUAWEI



# 目标

- 学完本课程后，您将能够:
  - 理解虚拟防火墙的技术原理
  - 掌握虚拟防火墙配置方法
  - 熟悉虚拟防火墙技术应用









# 目录

1. **虚拟防火墙技术介绍**
2. 虚拟防火墙技术原理
3. 虚拟防火墙应用分析







## 企业网络安全面临的问题

| 安全防护细化 | 安全业务隔离 | 业务应用多样 | 安全投资维护 |
| --- | --- | --- | --- |
| 网络环境日渐复杂，安全防护的要求越来越细化。 | 网络中业务应用越来越多，为保障业务数据安全，急需实现业务间的安全隔离。 | 单纯的物理网络隔离已经无法适应网络结构的复杂化和业务应用的多样化要求 | 越来越多的防火墙等安全设备布署，造成投资不断加大设备维护压力越来越大，负担越来越重 |



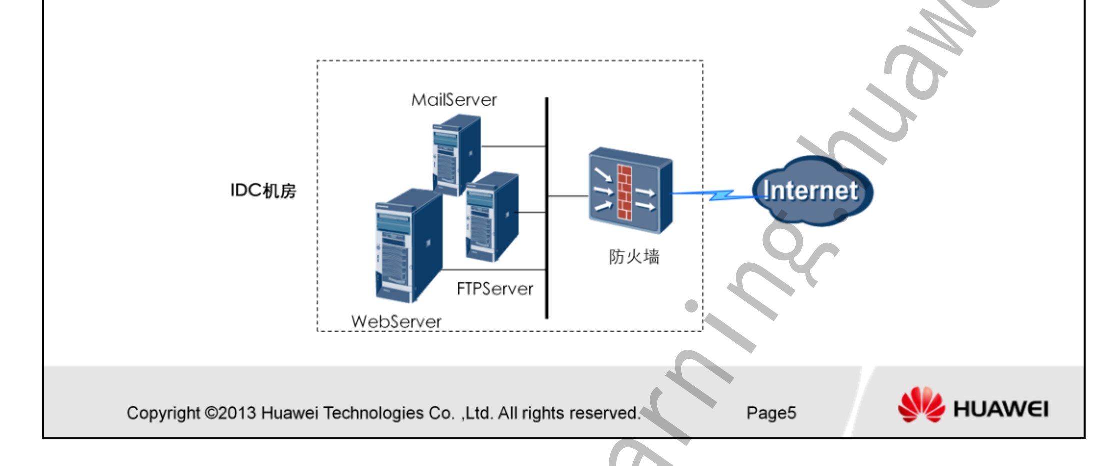





随着网络技术的普及，网络规模不断扩大，其应用和复杂度也在不断增加。对一个网络环境复杂的运营商网络或企业网来说，通常包括很多不同的省市/部门/群组，此时网络上承载着各种不同的复杂应用。很多时候，需要对这些不同部门/群组用户的访问权限进行控制、不同业务间的网络传输也需要安全隔离，这种隔离指的是访问、传输、应用端到端的隔离。

对于有业务和应用隔离需求的用户来说，传统的物理网络隔离无法满足需求；网络安全设备的大量重复采购，造成设备管理及安全策略的布署困难，大大增加了用户投资和网络建设、运维、管理方面的负担。为了达到隔离目的，同时节约投资成本，提出了单个防火墙作为多个防火墙来用的需求，虚拟防火墙技术应运而生。

虚拟防火墙技术是在一个物理防火墙设备上虚拟出多个逻辑上防火墙的技术。

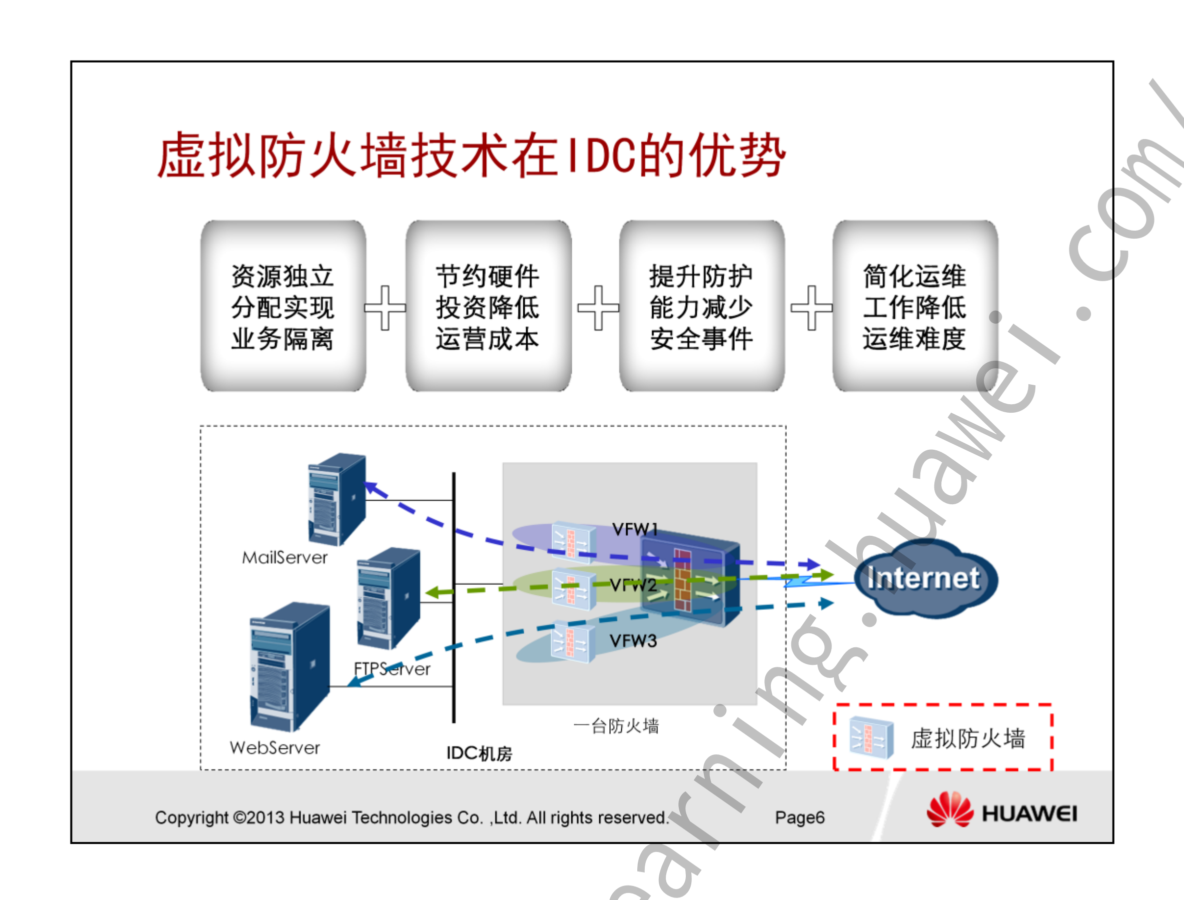



IDC（Internet Data Center互联网数据中心）主要为ICP（Internet Content Provider internet 内容提供商）、企业、媒体和各类网站提供大规模、高质量、安全可靠的专业化服务器托管、空间租用、网络批发带宽以及ASP（Active Server Pages 动态服务器网页）、EC(Electronic Commerce 电子商务)等业务。随着互联网规模的不断扩大，各种业务应用的服务器数量越来越庞大，IDC机房中越来越多的服务器需要安全防护。

传统防护方式是多台服务器前端放置一台防火墙，以保护服务器安全。如图所示。

在IDC机房中，并不是所有的服务器都会同时遭受外来黑客的攻击。通常，遭受攻击的仅是其中的某台服务器或其应用，例如WEB服务器、邮件服务器。一旦托管的某台服务器遭受攻击，防火墙会耗费大量系统资源来抗击黑客的攻击流量，由于防火墙处在网络出口节点，系统资源的大量消耗会严重影响其它服务器的正常应用，正所谓城门失火快及池鱼，势必导致IDC的服务质量大大降低。

而为每一台托管服务器配置一台防火墙，会造成托管成本大大提高，同时，大量布署的网络安全设备也会造成维护工作量持续增加，维护成本的不断提高。虚拟防火墙技术解决了以上一系列问题，在IDC得到较广泛的应用。

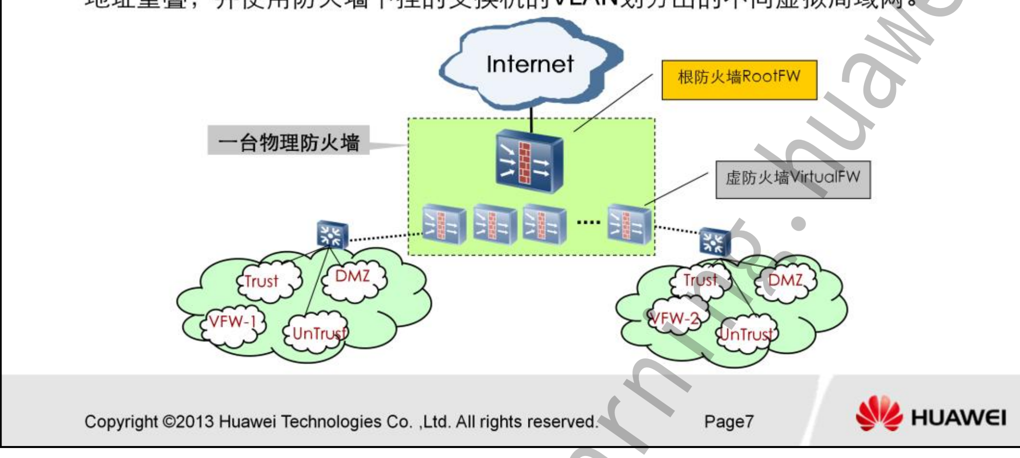




虚拟防火墙支持多实例解决方案，可以将一台防火墙从逻辑上划分为多台虚拟防火墙，分别为多个小型私有网络提供独立的安全保障。实现虚拟防火墙的传统方式是通过在接口上绑定VPN实例，将接口收到报文发送至相应的VPN实例中，每一个VPN实例即代表一个虚拟防火墙。当需要根据IP地址来区分属于不同虚拟防火墙的报文时，可以使用IP分流功能，将报文分流到相应的VPN实例（即虚拟防火墙）中。与在接口上绑定VPN实例的方式相比，IP分流功能的配置和使用更加简单，同时可以节省设备的接口资源。

系统资源都按业务规划分配到各个独立的虚拟防火墙，各个虚拟防火墙能够独立防御针对自己保护的服务器和应用的攻击，既使其中某个虚拟防火墙系统资源被网络攻击耗尽，也不会影响其他的虚拟防火墙系统，其它的服务器和应用仍然可以正常运行，保障了IDC运营的稳定性，大大提高了IDC整体服务质量；

虚拟防火墙技术上大大降低了防火墙硬件设备资金投入，用一台防火墙就可以达到多台防火墙防护水平；从托管用户方面来看，所属服务器相当于由一台独立的防火墙来保护，提升了安全防护能力，用户满意程度也会大幅提升，吸引更多托管用户，从而间接的增加了IDC的营业额；从IDC运营角度来说，网络管理员只需要对一台防火墙进行管理，达到对多台设备统一管理的目的，大大降低了管理难度，减少了维护的复杂度。




虚拟防火墙技术为运营商或大型企业提供虚拟防火墙租售服务，其中虚拟防火墙实例VFW1租给企业A，虚拟防火墙实例VFW2租给企业B，企业A和企业B可以地址重叠，并使用防火墙下挂的交换机的VLAN划分出的不同虚拟局域网。其中虚拟防火墙实例VFW1和实例VFW2均由根防火墙管理员进行创建，而各虚拟防火墙相关配置（如NAT多实例、VPN多实例等）由各虚拟防火墙管理员自行来配置，但各虚拟防火墙的管理员用户需根防火墙管理员事先创建。

- 利用虚拟防火墙技术，将一台防火墙逻辑上划分为两个虚拟防火墙VFW1、VFW2，分别租给企业A和企业B，为企业A和企业B提供安全防护；
- 系统为虚拟防火墙VFW1、VFW2分别提供独立的系统资源，之间互不影响；
- 对用户透明，企业A与企业B之间业务完全隔离，与使用分别单独布署防火墙一样；
- 企业A分为Trust、Dmz和Untrust区，其中trust为内部网络，Dmz区部署对外服务器，Untrust区拥有公网地址；企业B分为Trust、Dmz和Untrust区，其中Trust为内部网络，Dmz区提供对外服务器，Untrust区拥有私网地址。

通过虚拟防火墙的应用，有效的解决传统防火墙的不足，实现了灵活部属，简化了网络结构；管理员对各自的虚拟防火墙进行管理，互不影响，大大减轻了维护工作量；为运营商或企业减轻了投资，只需购买一台设备即可为不同用户提供各自的安全服务。

# 虚拟防火墙技术应用场景二

- VPN多实例业务

  两个VPN的出差用户，在公网通过RootVFW登录到私网的VPN中，并直接访问私网资源。

VPN-1的出差员工
Internet
VPN-2的出差员工
防火墙
RadiusServer
VPN-1
VPN-2
虚拟防火墙





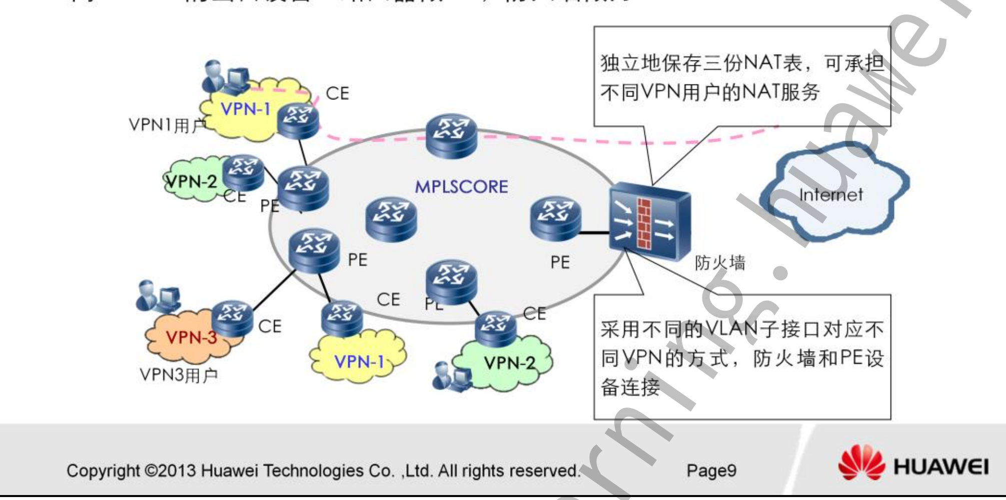
防火墙提供的VPN多实例业务具有如下一特点：

- 安全性高：VPN用户的接入是通过防火墙的验证和授权，接入之后的访问是采用独立的虚拟防火墙系统对用户进行管理。不同VPN用户的资源是完全隔离；
- VPN接入方式灵活可靠：可以支持从公网到VPN，也可以支持从VPN到VPN两种模式；
- 接入控制权限严格：防火墙可以根据用户名、密码来控制访问VPN的接入权限，这样可以使得出差员工、超级用户（需要访问不同VPN资源）等不同的用户具备不同的访问权限。

# 虚拟防火墙技术应用场景三

- MPLS网络与IP网络的无缝集成

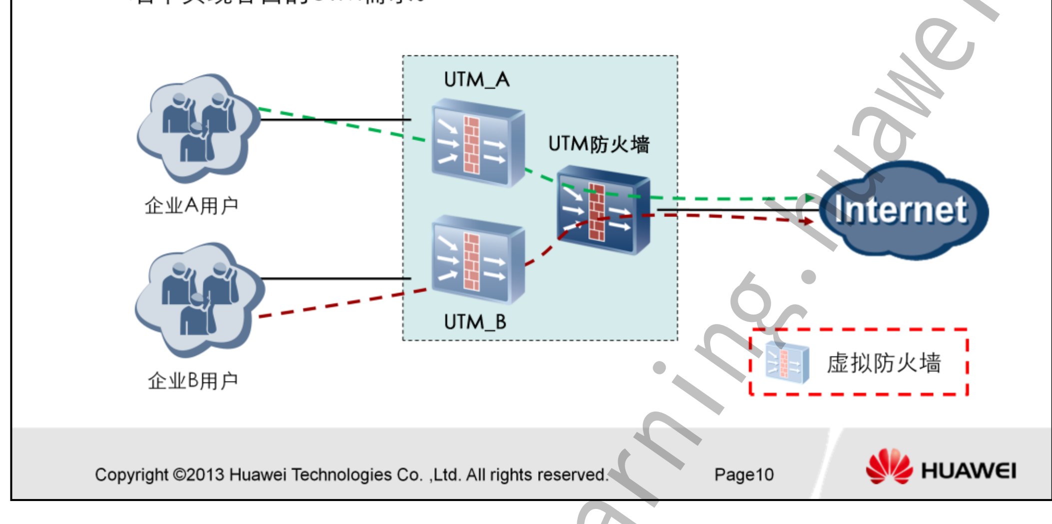
  防火墙放置在一个MPLS骨干网络的出口，做为一个MPLSVPN网络统一访问Internet的出口设备。路由器做PE，防火墙做为MCE。



利用虚拟防火墙、地址转换多实例、multi-VRF等VPN隔离技术，将防火墙放置在一个MPLS骨干网络的出口，做为一个MPLSVPN网络统一访问Internet的出口设备。在MPLS网络之外承担MCE（muti – CE）的功能，在防火墙的出入接口划分不同的VLAN或逻辑子接口，将不同的分支机构或不同的业务通过进出不同的VLAN或子接口进入不同的虚拟防火墙VPN实例，从而达到了隔离的目的，为MPLSVPN统一提供Internet访问。

- 支持完善的安全防范业务，可以避免来自Internet的攻击，保护整个MPLS网络的安全；
- 支持完善的VLAN、VRF、OSPF、BGP等技术，可以很好的解决MPLS网络和IP网络的融合问题；
- 支持业务多实例特性，资源独立存放，可以很好的解决私网地址重叠的问题。




UTM（Unified Threat Management）可以将多种安全功能集成于一个设备中，保护用户不受多种网络威胁的侵扰。

UTM虚拟化即在虚拟防火墙中配置UTM。通过绑定虚拟防火墙，可以在不同的虚拟防火墙上实现不同的UTM需求。在不同的虚拟防火墙上进行自定义配置支持公共模式组 、Web过滤、邮件内容过滤、FTP过滤和DPI。

但以下特性不支持在虚拟防火墙中进行自定义配置，只能使用根防火墙上的配置，包括IPS、AV、RBL、各类特征库（AV病毒库、IPS签名库、URL热点库、DPI知识库）。



# 目录









# 虚拟防火墙技术发展

- 虚拟防火墙技术实现经历了两个过程：
  - **转发多实例：**

    存在多张路由表、转发表，支持地址重叠，都在同一配置界面上实现，拥有配置权限的用户可以配置和查看所有的数据。
  - **转发多实例+配置多实例**

    某一实例下的用户只能查看和配置与自己相关的内容和信息，不能跨VPN查看和修改数据，具有超级用户权限的用户除外。







虚拟防火墙是在一个物理防火墙设备上虚拟出多个逻辑上防火墙，其核心内容是能够支持转发多实例，即支持多张路由表支持地址重叠等内容。

转发多实例+配置多实例的实现能带来一个好处，即在组网划分完之后，系统管理员可以将各VPN交给各VPN管理员，系统管理员不再关心各VPN细节。这样能使实现组网配置的分级管理以及VPN出租业务，VPN出租后由用户自己管理，既带来了管理的方便性又节约了维护成本。

目前，转发多实例+配置多实例方式已经成为现在业界主流的虚拟防火墙实现技术。

## 虚拟防火墙技术原理

- 虚拟防火墙都是VPN实例（VPN-Instance）、安全实例和配置实例等的综合体。
- 虚拟防火墙提供如下多实例：
  - VPN多实例
  - 安全多实例
  - 配置多实例
  - NAT多实例
  - 路由多实例
  - UTM多实例









每个虚拟防火墙都是VPN实例（VPN-Instance）、安全实例和配置实例的综合体，能够为虚拟防火墙用户提供私有的路由转发平面、安全服务和配置管理平面。

- **VPN实例**

VPN实例为虚拟防火墙提供相互隔离的VPN路由，与虚拟防火墙相关的信息主要包括：VPN路由以及与VPN实例绑定的接口。VPN路由将为转发来自与VPN实例绑定的接口的报文提供路由支持。VPN实例与虚拟防火墙是一一对应的。

- **安全实例**

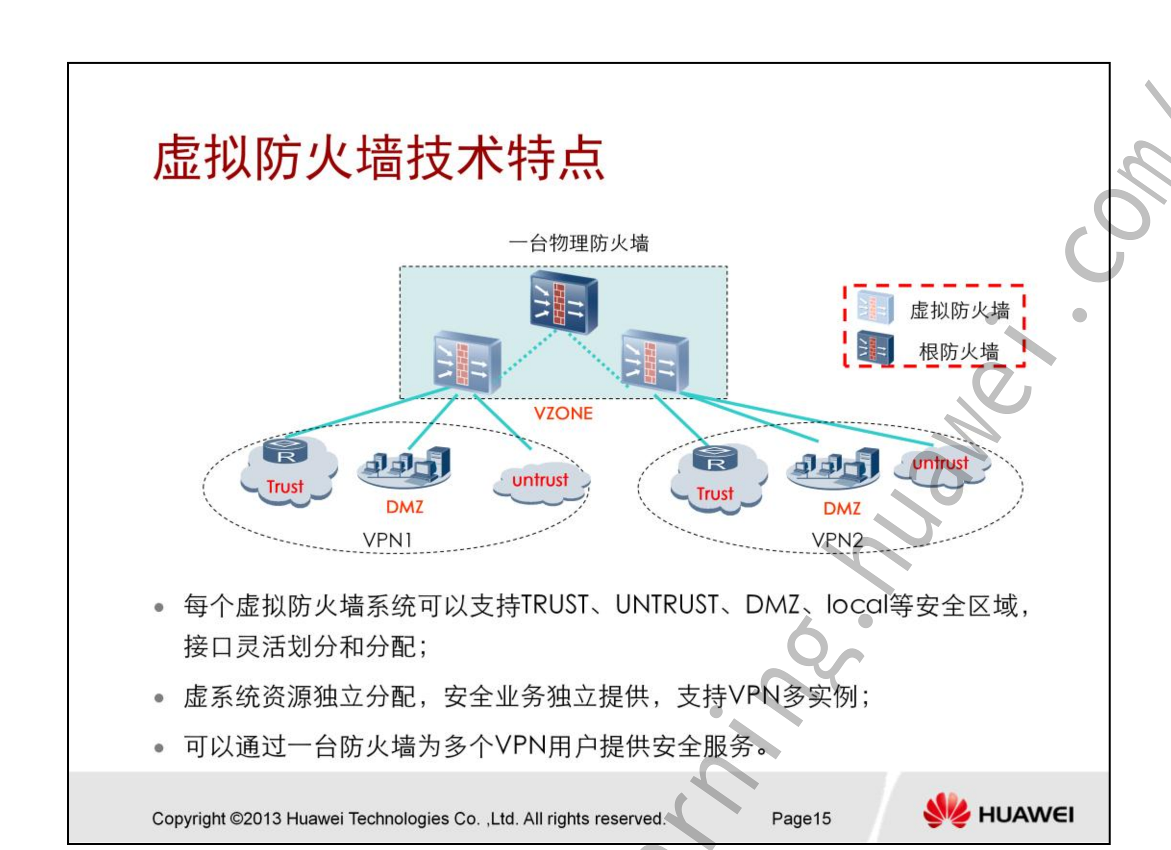
安全实例为虚拟防火墙提供相互隔离的安全服务，同样与虚拟防火墙一一对应。安全实例具备私有的区域、域间、ACL规则组和NAT地址池，并且能够将绑定接口加入私有区域；安全实例能够为虚拟防火墙提供地址绑定、黑名单、地址转换、包过滤、统计、攻击防范、ASPF和NATALG等私有的安全服务。

- **配置实例**

配置实例为虚拟防火墙用户提供相互隔离的配置管理平面，与虚拟防火墙是一一对应。虚拟防火墙用户登陆防火墙后有权管理和维护私有的VPN路由和安全实例。创建虚拟防火墙后，逻辑上，防火墙将分为两类：根防火墙（Root-firewall,Rfw）和虚拟防火墙。根防火墙对应于未配置虚拟防火墙功能的防火墙，并和所有虚拟防火墙构成超级防火墙（Super-firewall,Sfw）。超级防火墙用户有权管理根防火墙和所有虚拟防火墙。

- **NAT实例**

NAT实例为虚拟防火墙用户提供相互隔离的NAT服务，与虚拟防火墙一一对应。




为了和创建的虚拟防火墙区别，设备本身称为根防火墙。在创建虚拟防火墙之后，需要配置接口绑定虚拟防火墙并加入其安全域，再配置虚拟防火墙的相关包过滤策略及路由，以实现虚拟防火墙内部的基本通信。若要实现虚拟防火墙和根防火墙之间的通信，则还需配置二者之间的包过滤策略以及路由。

**虚拟防火墙技术特点：**

提供路由多实例、安全多实例、配置多实例、NAT多实例、VPN多实例，应用灵活，可满足多种组网需要。

每个虚拟防火墙均可以独立支持TRUST、UNTRUST、DMZ、LOCAL等4个安全区域（USG5000系列支持VZONE区域，通过VZONE区域实现虚拟防火墙之间的互访），接口灵活划分和分配。

资源独立分配，每个虚系统的转发表项等资源是独立分配的，从技术上保证了每一个虚系统和一个独立防火墙从实现上是一样的，而且非常安全，各个虚系统之间是无法直接访问。只有在虚系统之间引入了对方的路由，才可以使得虚系统之间可以通信。

所有的安全业务都可以针对虚系统独立配置。例如，包过滤、NAT、攻击防范等等。这样在用户使用虚系统服务的时候，也可以同时享受防火墙所能提供的各种安全业务。

每个虚系统提供独立的管理员权限，针对虚系统的管理员只能管理本虚系统的相关配置，也只能看到自己虚系统的配置。对虚系统管理员而言，他只能看见一个虚拟独立的防火墙配置。

USG9300系列最大提供1024个虚拟防火墙，其它设备（USG5000系列、USG3000系列）均可提供100个虚拟防火墙，提供了灵活可靠的组网保障。

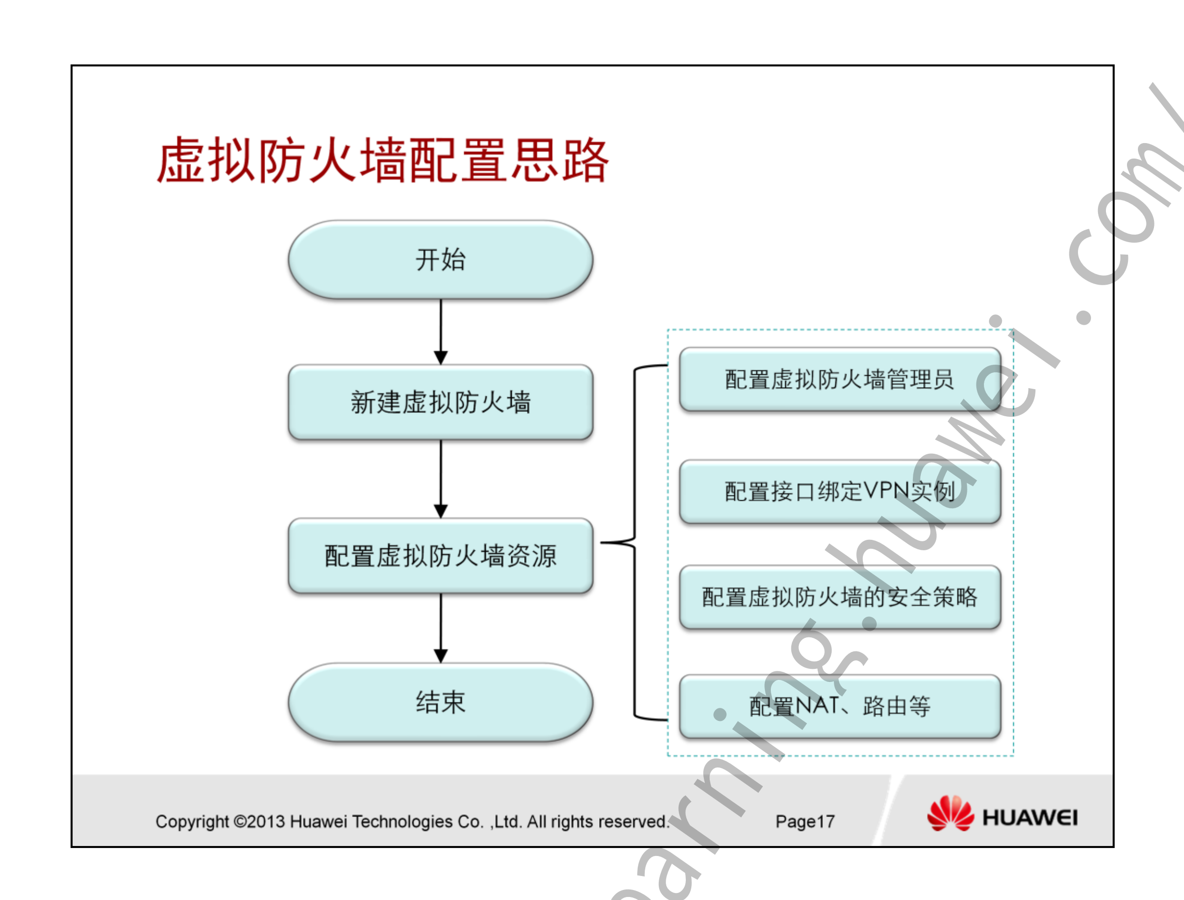


# 目录








虚拟防火墙配置思路：

①配置定义多实例－>②多实例和接口绑定－>③将接口分别加入域－>④配置虚拟防火墙的内部的域间包过滤和路由，以实现虚拟防火墙的内部的基本通信－> ⑤若需实现根防火墙和虚拟防火墙之间的通信，请配置二者之间的域间包过滤和静态路由

- 虚拟防火墙由超级用户创建，创建步骤包括：
  - 定义VPN实例；
  - 配置接口与VPN实例的绑定；
  - 配置本地用户与VPN实例的绑定。

## 虚拟防火墙配置步骤（1）

- 创建/删除VPN实例
  - 创建/删除VPN实例

[*undo*] **ip vpn-instance** *vpn-instance-name* [*vpn-id vpn-id*]

- 为VPN实例指定路由标识
  - 为VPN实例指定路由标识

**route-distinguisher** *vpn-route-distinguisher*








缺省情况下，未创建虚拟防火墙。

在执行ip vpn-instance命令时，如果相应的虚拟防火墙已经创建，则可以直接配置ip vpn-instance vpn-instance-name进入该虚拟防火墙视图；否则，必须配置vpn-id后，才能进入虚拟防火墙视图。

USG5000防火墙支持100个虚拟防火墙，虚拟防火墙ID范围为1～100，可提供99个VFW配置。

RD用于区分使用相同地址空间的IPv4前缀，不能用于判断某条路由的发起者，也不能判断某条路由属于哪个VPN。服务供应商可以独立地分配RD，但必须保证RD全局唯一。这样，即使来自不同服务提供商的VPN使用了相同的IPv4地址空间，防火墙也可以向各VPN发布不同的路由。当防火墙收到私网路由后，为实现私网路由的独立性，需要将这些私网路由附加RD后引入到公网路由表中。当RD为全0时，表示该IPv4路由是普通路由。

**注意：**

1）创建VPN实例后，需要为该VPN实例指定路由标识，否则不能进行后续配置；

2）虚拟防火墙的ID不能重叠。

# 虚拟防火墙配置步骤（2）

- 配置接口绑定VPN实例
  - 配置接口与VPN实例的绑定

    **Ip binding vpn-instance** *vpn-instance-name*
  - 取消接口与VPN实例的绑定

    *Undo* **ip binding vpn-instance** *vpn-instance-name*
  - 缺省情况下，未配置接口与VPN实例之间的绑定。
  - 配置举例：

```
[USG5000]interface ethernet4/0/1
[USG5000-Ethernet4/0/1]ip binding vpn-instance vfw1
[USG5000-Ethernet4/0/1]ip address192.168.1.1255.255.255.0
```






配置接口时，需要首先配置接口绑定VPN实例，再配置接口IP地址。如果顺序相反，最初配置的接口IP地址会被删除，需要重新配置。

# 虚拟防火墙配置步骤（3）

- 配置接口加入安全域
  - 进入VPN实例的安全区域视图

    **Firewall zone** [ **vpn-instance** *vpn-instance-name*] [**name**] *zone-name*

  - 配置安全区域的安全级别

    **Set priority** *security-priority*

  - 配置接口加入安全区域

    **Add interface** *interface-type interface-number*

  - 缺省情况下，接口未加入安全域。








注意事项：

- 创建一个VPN实例的安全区域后，需要设置它的安全级别；
- 配置接口加入安全区域时，需要保证接口与安全区域同属于一个VPN实例。

# 虚拟防火墙配置步骤（4）

- 配置域间转发策略
  - 进入VPN实例的域间防火墙策略视图

    **Policy inter zone vpn-instance** *vpn-instance-name zone-name1 zone-name2* {**inbound**|**outbound**}

  - 创建并进入策略ID视图

    **Policy** [*policy-id*]

  - 指定防火墙策略的源地址

    **Policy source** {*source-address{source-wildcard*|*0*|*mask{mask-address*|*mask-len}}*|*address-set{address-set-name}*<1-256>|*range begin-addressend-address* |*any*}







进入虚拟防火墙的各安全区域后，转发策略同在根防火墙上配置相似。

# 虚拟防火墙配置步骤（5）

- 指定防火墙策略的目的地址

  **Policy destination {***destination-address {destination-wildcard|0|mask {mask-address |mask-len}}|address-set {address-set-name}&<1-256>|range begin-addres send-address |any* }

- 指定防火墙策略的服务集

  **Policy service** *service-set{service-set-name}&<1-256>*

- 配置防火墙策略的动作

  **Action** { **permit** | **deny** }

• 配置虚拟防火墙内部转发报文的路由

  **ip route-static vpn-instance** *vpn-instance-name* ***destenation-address*** { *mask* | *mask-length* } ***nexthop-address***








若需实现根防火墙和虚拟防火墙之间的通信，需要配置二者之间的域间包过滤和静态路由。

# 虚拟防火墙配置步骤（6）

- 配置根防火墙和虚拟防火墙之间的通信
  - 进入根防火墙的Trust和虚拟防火墙VPN1的Untrust域间

**policy interzone** *trust* **vpn-instance** vpn1 untrust **inbound**

  - 配置根防火墙的Trust和虚拟防火墙VPN1转发策略（略）
  - 配置根防火墙向VPN1转发报文的路由

**ip route-static destination-address** { mask | mask-length } **vpn-instance** *VPN1 nexthop-address*

  - 配置VPN1向根防火墙转发报文的路由

**ip route-static vpn-instance** *VPN1 destination-address* { mask | mask-length } *nexthop-address* **public**

或**ip route-static vpn-instance** *VPN1 destination-address* { mask | mask-length } *interface-type interface-number* [ *nexthop-address* ]






# 配置虚拟防火墙管理员

- 执行命令aaa，进入AAA视图。
- 创建用户

```
local-user user-name password cipher password
```

- 配置本地用户与虚拟防火墙的绑定

```
local-user user-name vpn-instance vpn-instance-name
```

- 对指定用户配置服务类型。

```
local-user user-name service-type { ssh | telnet | web }
```

  - 与虚拟防火墙绑定的本地用户仅支持SSH，Telnet，Web服务类型。
- 配置用户的优先级

```
local-user user-name level level
```







根防火墙的用户可以通过console、web、telnet、SSH方式配置和管理根防火墙和所有虚拟防火墙。

虚拟防火墙的用户只能通过web、telnet、SSH方式配置和管理其所属的虚拟防火墙。

## 透明模式虚拟防火墙配置

- 透明模式虚拟防火墙所有接口为二层接口，需配置VLAN与VPN绑定，配置如下：
  - 创建VLAN并进入VLAN视图

```
Vlan vlan-id
```

  - 将VLAN和VPN实例绑定

```
Binding vpn-instance vpn-instance-name
```

  - 进入以太网接口视图，设置端口所属的缺省VLAN

```
Interface interface-type interface-number
Port default vlan vlan-id
```

  - 其他配置与路由模式相同。






透明模式的虚拟防火墙通过将VLAN和虚拟防火墙进行一一绑定，实现网络中同一网段地址的相互隔离。

透明模式的虚拟防火墙使处在同一网段相同VLAN中的地址能相互访问，不同VLAN中的不能访问。当两个不同VLAN网络中存在相同IP时，根防火墙不能实现对同一IP采用不同的安全策略，故通过配置透明模式的虚拟防火墙可以将两个VLAN绑定到不同的虚拟防火墙，从而实现对该场景的支持。

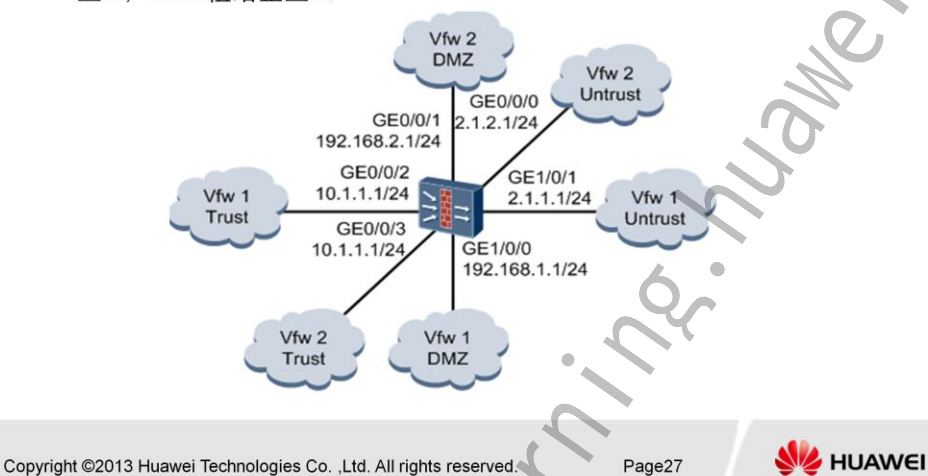


# 目录








企业A和企业B能够地址重叠；

两个私有网络均分别划分为Trust、DMZ（Demilitarized Zone）、Untrust三个安全区域。其中，Trust安全区域部署内部用户，DMZ安全区域部署对外服务器，Untrust安全区域部署外部用户；

Trust安全区域内的用户通过公网地址访问外部网络；

Untrust安全区域的用户能够访问DMZ安全区域的服务器。

# 虚拟防火墙配置实例（1）

- 在根防火墙上配置基本UTM过滤：（以IPS签名库配置为例）
- 配置运行模式为UTM

  [USG] runmode utm
- 启用IPS功能，并配置IPS工作模式为protective使阻断响应生效。

  [USG] ips enable

  [USG] ips mode protective
- 配置IPS策略。（略）






IPS策略配置配置参考命令:

创建IPS策略protecthttp:

[USG] **ips policy protecthttp**

[USG-ips-policy-protecthttp] **signature-set abc**

[USG-ips-policy-protecthttp-signset-abc] **direction enable**

[USG-ips-policy-protecthttp-signset-abc] **direction to-server**

[USG-ips-policy-protecthttp-signset-abc] **severity enable**

[USG-ips-policy-protecthttp-signset-abc] **severity above critical**

[USG-ips-policy-protecthttp-signset-abc] **protocol enable**

[USG-ips-policy-protecthttp-signset-abc] **protocol http**

[USG-ips-policy-protecthttp-signset-abc] **signature-set enable**

[USG-ips-policy-protecthttp-signset-abc] **signature-set action block**

应用IPS策略:

[USG] **policy interzone dmz untrust inbound**

[USG-policy-interzone-dmz-untrust-inbound] **policy 0**

[USG-policy-interzone-dmz-untrust-inbound-0] **action permit**

[USG-policy-interzone-dmz-untrust-inbound-0] **policy ips protecthttp**

# 虚拟防火墙配置实例（2）

- 完成企业A的配置
  - 创建VPN实例vfw1

[USG5000]ip vpn-instance vfw1 vpn-id1

[USG5000-vpn-vfw1]route-distinguisher 100:1

  - 配置接口绑定到Vfw1

[USG5000]interface GigabitEthernet0/0/2

[USG5000-GigabitEthernet0/0/2]ip binding vpn-instance vfw1

[USG5000-GigabitEthernet0/0/2]ip address10.1.1.124

  - GigabitEthernet1/0/0、GigabitEthernet1/0/1配置略








创建VPN实例后，需要同时配置路由标识，否则不能进行后续配置；

需要首先配置接口与VPN实例的绑定，再配置接口IP地址。如果配置顺序相反，先配置的地址会被删除；

接口与安全区域需要均属于同一VPN实例，否则无法成功将接口加入安全区域。

企业B的相应配置为：

**#创建VPN实例vfw2**

[USG5000]ip vpn-instance vfw2 vpn-id2

[USG5000-vpn-vfw1]route-distinguisher 100:2

**#配置接口绑定到Vfw2**

[USG5000]interface GigabitEthernet0/0/3

[USG5000-GigabitEthernet0/0/3]ip binding vpn-instance vfw2

[USG5000-GigabitEthernet0/0/3]ip address10.1.1.124

**#GigabitEthernet1/0/0、GigabitEthernet1/0/1配置略**

# 虚拟防火墙配置实例（3）

- 配置接口加入安全域

[USG5000]firewall zone vpn-instance vfw1 trust

[USG5000-zone-trust-vfw1]add interface GigabitEthernet0/0/2

[USG5000]firewallzonevpn-instance vfw1 dmz

- GigabitEthernet1/0/0、GigabitEthernet1/0/1配置略

- 配置Trust安全区域的用户可以通过公网地址访问外部网络
  - 配置NAT地址池

USG5000]nat address-group12.1.1.5  2.1.1.10 vpn-instance vfw1








企业B相应配置为:

#配置接口加入安全域

[USG5000]firewall zone vpn-instance vfw2 trust

[USG5000-zone-trust-vfw2]add interface GigabitEthernet0/0/3

#GigabitEthernet0/0/0、GigabitEthernet0/0/1配置略

配置Trust安全区域的用户可以通过公网地址访问外部网络

#配置NAT地址池

USG5000]nat address-group 12.1.2.5  2.1.2.10 vpn-instance vfw2

## 虚拟防火墙配置实例（4）

- 配置Trust到Untrust域间出方向的防火墙策略

[USG5000]policy interzone vpn-instance vfw1 trust untrust outbound

[USG5000-policy-interzone-trust-untrust-vfw1-outbound]policy1

[USG5000-policy-interzone-trust-untrust-vfw1-outbound-1]policy source 10.1.1.0 0.0.0.255

[USG5000-policy-interzone-trust-untrust-vfw1-outbound-1]action permit

- 配置Trust到Untrust域间出方向的NAT策略

[USG5000]nat-policy interzone vpn-instance vfw1 trust untrust outbound

[USG5000-nat-policy-interzone-trust-untrust-vfw1-outbound]policy1

[USG5000-nat-policy-interzone-trust-untrust-vfw1-outbound-1]policy source 10.1.1.0 0.0.0.255

[USG5000-nat-policy-interzone-trust-untrust-vfw1-outbound-1]action source-nat

[USG5000-nat-policy-interzone-trust-untrust-vfw1-outbound-1]address-group1







企业B相应配置为:

**#配置Trust到Untrust域间出方向的防火墙策略**

[USG5000]policy interzone vpn-instance vfw2 trust untrust outbound

[USG5000-policy-interzone-trust-untrust-vfw2-outbound]policy1

[USG5000-policy-interzone-trust-untrust-vfw2-outbound-1]policy source 10.1.10 0.0.0.255

[USG5000-policy-interzone-trust-untrust-vfw2-outbound-1]action permit

**#配置Trust到Untrust域间出方向的NAT策略**

[USG5000]nat-policy interzone vpn-instance vfw2 trust untrust outbound

[USG5000-nat-policy-interzone-trust-untrust-vfw2-outbound]policy1

[USG5000-nat-policy-interzone-trust-untrust-vfw2-outbound-1]policy source 10.1.10.0 0.0.0.255

[USG5000-nat-policy-interzone-trust-untrust-vfw2-outbound-1]action source-nat

[USG5000-nat-policy-interzone-trust-untrust-vfw2-outbound-1]address-group1

## 虚拟防火墙配置实例（5）

- 配置外部网络用户可以访问内部服务器
  - 配置vfw1的内部服务器

[USG5000]nat server zone vpn-instancevfw1untrust global 2.1.1.100 inside 192.168.1.2 vpn-instance vfw1

  - 配置vfw1的DMZ和Untrust域间防火墙策略

[USG5000]policy interzone vpn-instance vfw1 dmz untrust inbound

[USG5000-policy-interzone-dmz-untrust-vfw1-inbound]policy1

[USG5000-policy-interzone-dmz-untrust-vfw1-inbound-1]policy destination 192.168.1.2 0

[USG5000-policy-interzone-dmz-untrust-vfw1-inbound-1]action permit






企业B相应配置为:

**#配置vfw2的内部服务器**

[USG5000]nat server zone vpn-instance vfw2 untrust global 2.1.2.100 inside 192.168.2.2 vpn-instance vfw2

此处的内部服务器应属于VPN实例vfw2。

**#配置vfw2的DMZ和Untrust域间防火墙策略**

[USG5000]policy interzone vpn-instance vfw2dmz untrust inbound

[USG5000-policy-interzone-dmz-untrust-vfw2-inbound]policy1

[USG5000-policy-interzone-dmz-untrust-vfw2-inbound-1]policy destination 192.168.2.20

[USG5000-policy-interzone-dmz-untrust-vfw2-inbound-1]action permit

# 虚拟防火墙配置实例（6）

- 配置企业A的UTM过滤规则：（以FTP过滤为例，禁止下载文件类型为AVI的文件）

  [USG] ftp-filter policy ftppolicy vpn-instance a

  [USG-ftp-filter-policy-ftppolicy-a] download file-type group download action block

- 在域间应用UTM策略：

  [USG] policy interzone vpn-instance a trust untrust outbound

  [USG-policy-interzone-trust-untrust-a-outbound] policy 0

  [USG-policy-interzone-trust-untrust-a-outbound-0] action permit

  [USG-policy-interzone-trust-untrust-a-outbound-0] policy ips ips

  [USG-policy-interzone-trust-untrust-a-outbound-0] policy ftp-filter ftppolicy








公共策略组配置参考命令：

创建文件扩展名模式组download，将关键字AVI加入到公共模式组中。

[USG] pattern-group download type file-extension vpn-instance a

[USG-pattern-group-fe-download-a] pattern avi

[USG-pattern-group-fe-download-a] quit

[USG] pattern configure commit

企业B相应配置为：

配置企业B的UTM过滤规则：

[USG] ftp-filter policy ftppolicy vpn-instance b

[USG-ftp-filter-policy-ftppolicy-a] download file-type group download action block

在域间应用UTM策略：

[USG] policy interzone vpn-instance b trust untrust outbound

[USG-policy-interzone-trust-untrust-a-outbound] policy 0

[USG-policy-interzone-trust-untrust-a-outbound-0] action permit

[USG-policy-interzone-trust-untrust-a-outbound-0] policy ips ips

[USG-policy-interzone-trust-untrust-a-outbound-0] policy ftp-filter ftppolicy



# 总结

- 虚拟防火墙的技术原理
- 虚拟防火墙配置方法
- 虚拟防火墙技术应用









- 虚拟防火墙的技术原理是什么?
- 在配置虚拟防火墙时需要注意的是什么?






虚拟防火墙的技术原理是什么?

答题要点：虚拟防火墙是在一个物理防火墙设备上虚拟出多个逻辑上防火墙。其核心内容是能够支持转发多实例。可以将多张路由表、转发表，支持地址重叠，都在同一配置界面上实现，拥有配置权限的用户可以配置和查看所有的数据。

在配置虚拟防火墙时需要注意的是什么?

答题要点：配置虚拟防火墙相关参数时，需要在命令行中增加vpn-instance指定需要进入的虚拟防火墙。



- 判断题

  1.没有虚拟防火墙管理员的概念，对虚拟防火墙的管理只能由根防火墙管理进行统一管理。

  2.虚拟防火墙A与虚拟防火墙B之间可以实现业务交互，但虚拟防火墙不能与根防火墙实现业务交互。








习题与答案：

1、没有虚拟防火墙管理员的概念，对虚拟防火墙的管理只能由根防火墙管理进行统一管理。

答案：错误

2、虚拟防火墙A与虚拟防火墙B之间可以实现业务交互，但虚拟防火墙不能与根防火墙实现业务交互。

答案：错误

Thank You

www.huawei.com


HC120310005
防火墙VPN高级应用
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



# 目标

- 学完本课程后，您将能够：
  - 掌握IPSec VPN高级特性及配置
  - 掌握L2TP over IPSEC VPN高级特性及配置
  - 掌握SSL VPN双机热备应用场景







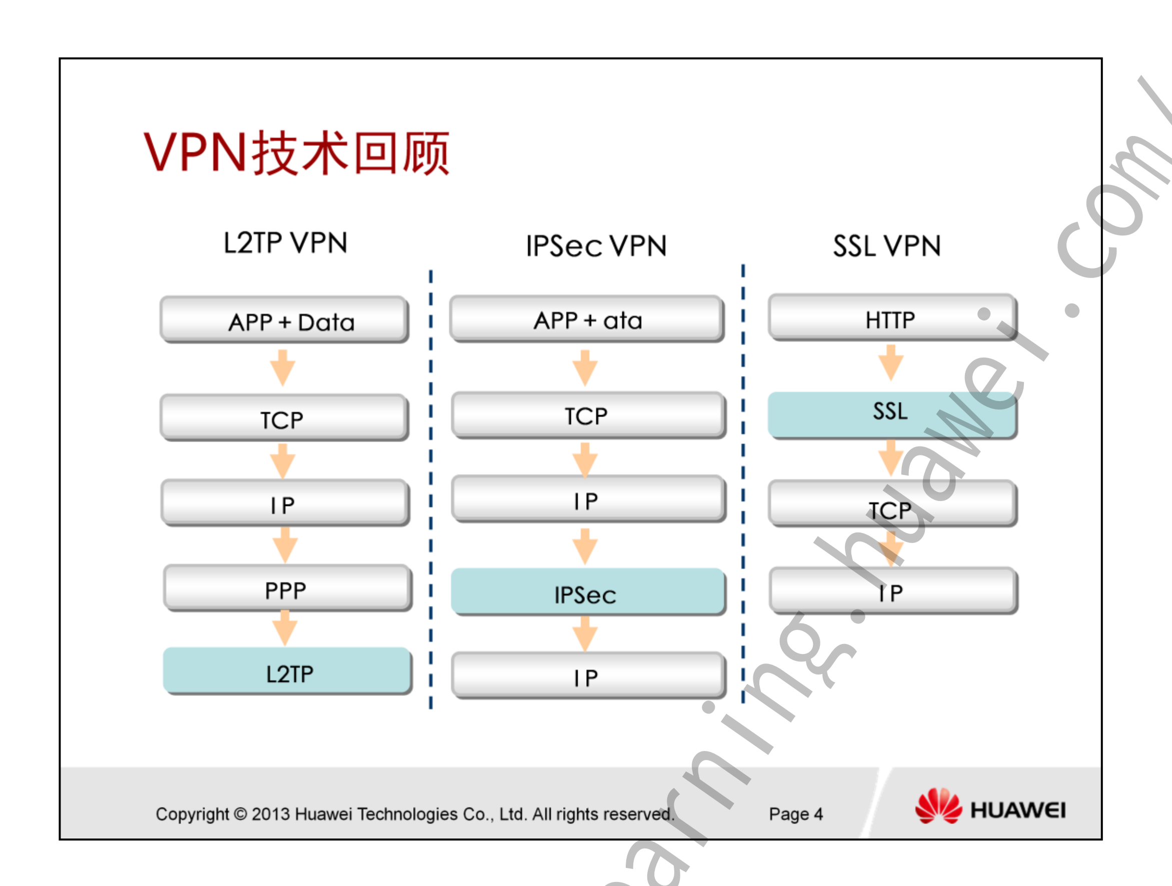

# 目录



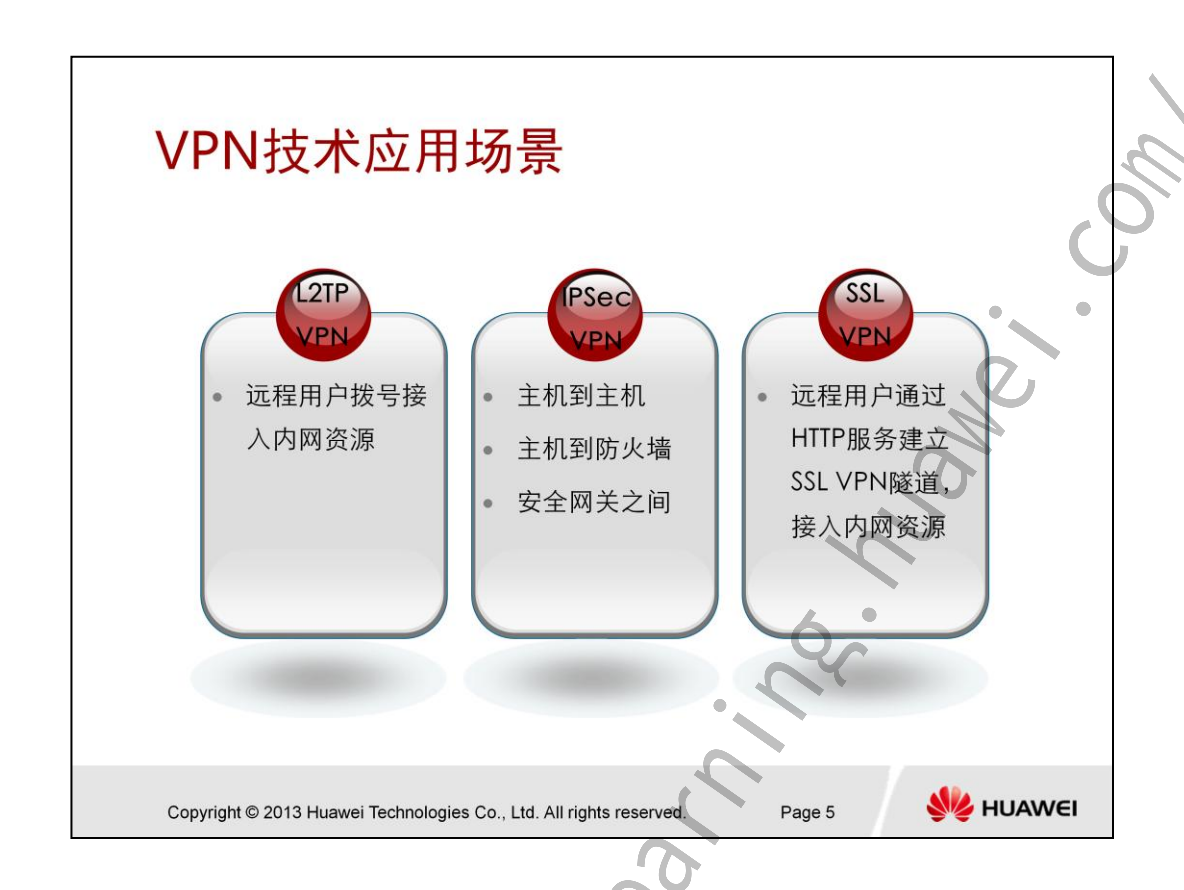









L2TP VPN封装了PPP协议，为二层VPN技术；IPSec VPN封装网络层协议，为三层VPN技术；SSL VPN主要为应用层HTTP协议进行保护。




IPSce VPN应用场景主要由以下三种类型：

- 网关（如防火墙）之间

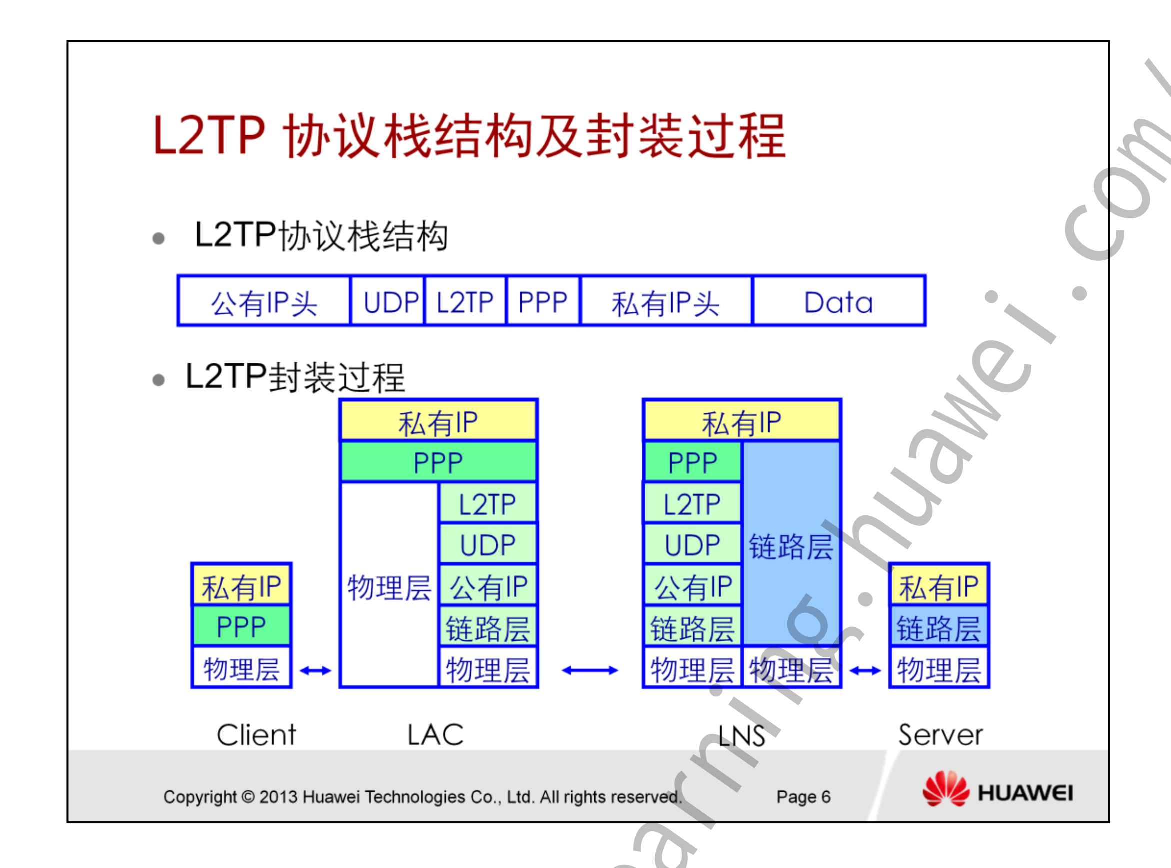
此种应用场景也叫点到点或点到多点IPSec VPN，主要用于公司总部与分支机构之间建立IPSec隧道，从而实现局域网之间互通。

- 主机与网关之间

主要用于出差员工通过互联网需要访问总部资源时。

- 主机与主机之间

主机之间通过互联网进行数据传输，需要加密时，加解密操作在主机侧完成。某些场景中，例如服务器放在DMZ区域，防火墙配置NAT server,也可以实现





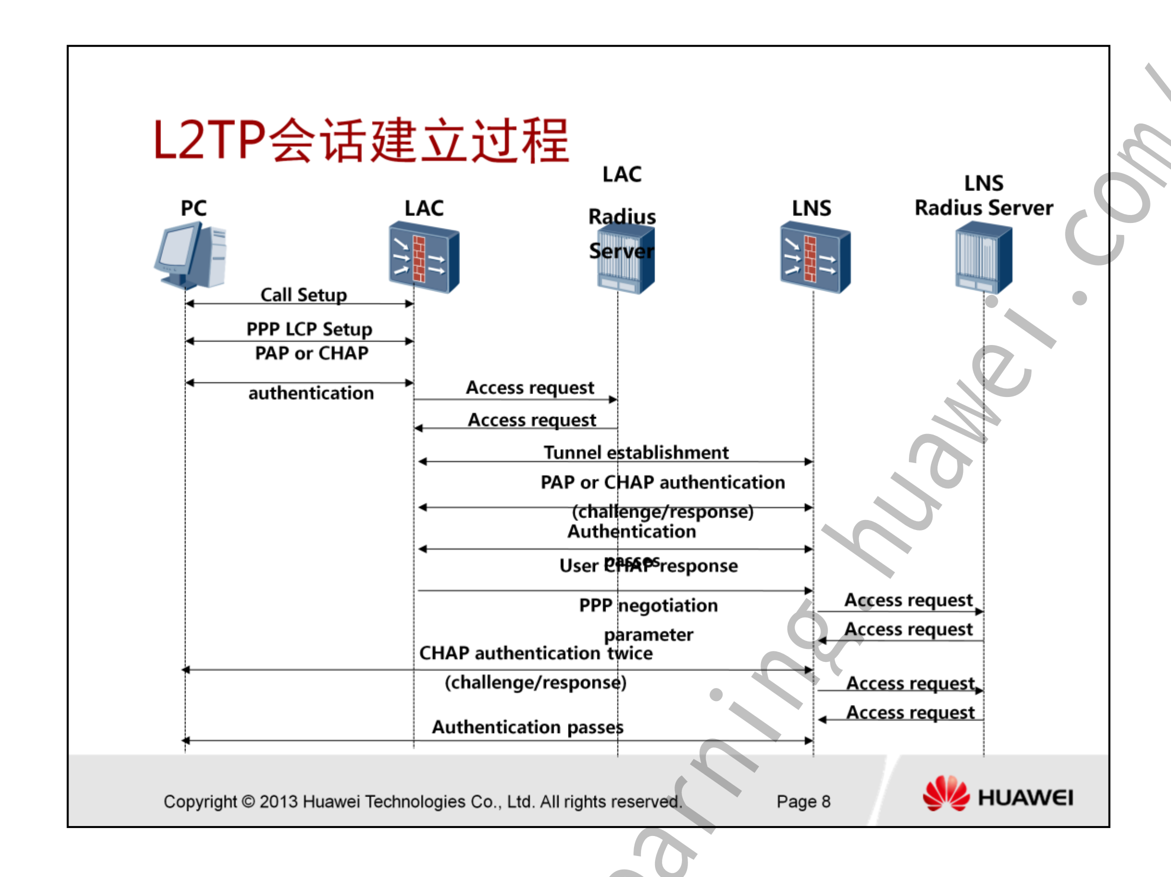
L2TP为什么是二层VPN协议？在L2TP VPN协议报文头中，其内封装了PPP报文。

LAC封装来自Client的PPP报文时，封装过程如下：

1. 封装L2TP头：其中包含了用于标识该消息的Tunnel ID和Session ID，这两个ID信息都是Remote端的ID而不是本地ID信息。
2. 封装UDP头：用于标识上层应用，L2TP注册了UDP 1701端口，当LNS收到了该端口的报文时能够辨别出这是L2TP报文从而送入L2TP处理模块进行处理。
3. 封装公网IP头：用于该报文在IP网（Internet）转发，注意LAC使用L2TP隧道的起点和终点地址来封装公网IP头.

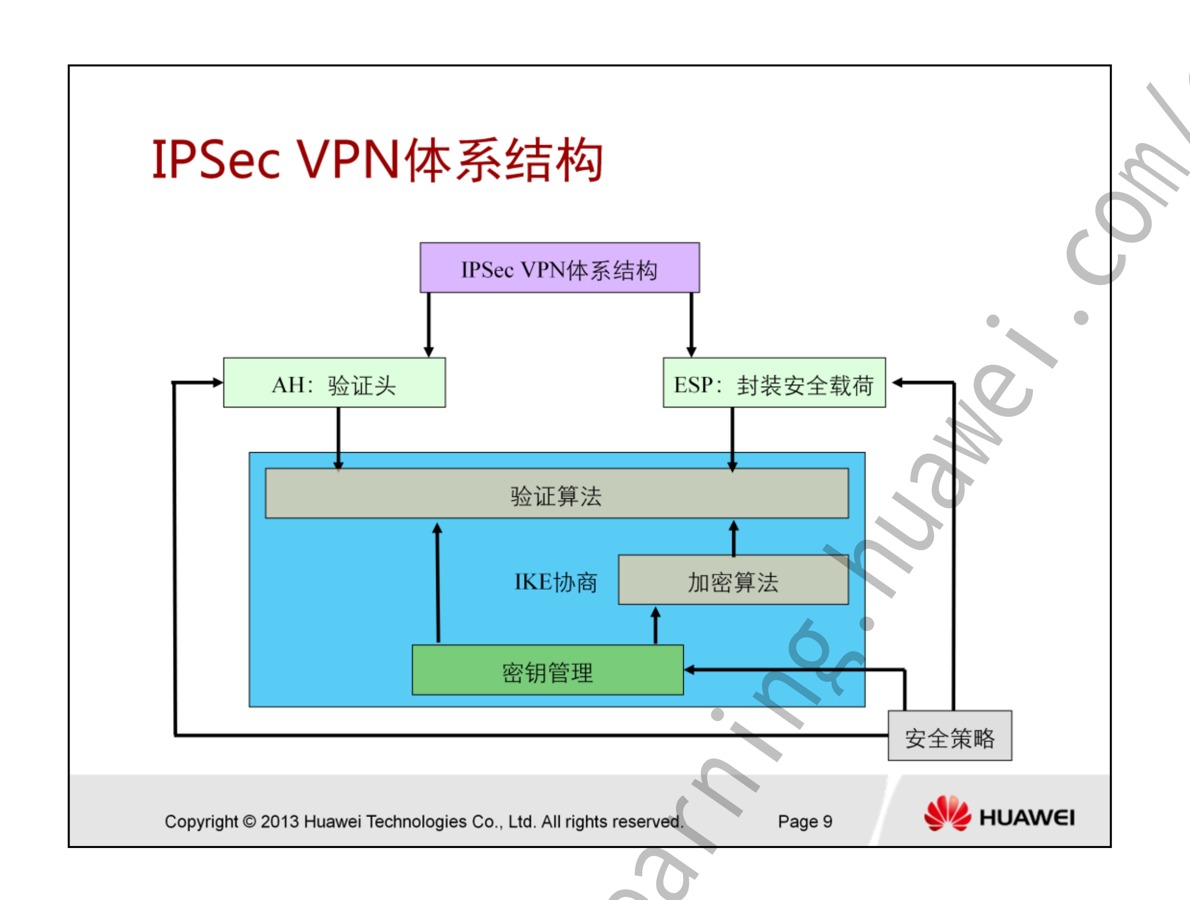
LNS收到L2TP报文以后，解封装过程如下：

1. 检查公网IP头和UDP头信息：LNS首先通过UDP端口标识该报文为L2TP报文，然后检查公网IP头的源目的地址是否和本地已经建立成功的L2TP隧道源目的地址相同，如果相同则解封装公网IP头和UDP头，否则丢弃报文。
2. 检查L2TP头信息：LNS读取L2TP头中的Tunnel ID和Session ID信息，检查其是否和本地已经建立成功的L2TP Tunnel ID和L2TP Session ID相同，如果相同则解封装，否则丢弃报文。
3. 检查PPP头信息：LNS检查PPP头中的相关信息是否正确，然后解封装PPP头。
4. 得到私网IP报文：此时LNS处理报文的过程就和收到一个普通的IP报文处理过程一致，将私网IP报文送入上层模块或者进行路由处理。




L2TP会话建立过程:

1. 用户端PC机发起呼叫连接请求。
2. PC机和LAC端进行PPP LCP协商。
3. LAC对PC机提供的用户信息进行PAP或CHAP认证。
4. LAC将认证信息（用户名、密码）发送给RADIUS服务器进行认证。
5. RADIUS服务器认证该用户，如果认证通过则返回该用户对应的LNS地址等相关信息，并且LAC准备发起Tunnel连接请求。
6. LAC端向指定LNS发起Tunnel连接请求。
7. LAC端向指定LNS发送CHAP challenge 信息，LNS回送该challenge响应消息CHAPresponse，并发送LNS 侧的CHAP challenge，LAC返回该challenge的响应消息CHAPresponse。
8. 隧道验证通过。
9. LAC端将用户CHAP response、response identifier和PPP协商参数传送给LNS。
10. LNS将接入请求信息发送给RADIUS服务器进行认证。
11. RADIUS服务器认证该请求信息，如果认证通过则返回响应信息。
12. 若用户在LNS侧配置强制本端CHAP认证，则LNS对用户进行认证，发送CHAP challenge，用户侧回应CHAP response。




IPSec VPN体系结构主要由AH、ESP和IKE协议套件组成。IPSec通过ESP来保障IP数据传输过程的机密性，使用AH/ESP提供数据完整性、数据源验证和抗报文重放功能。ESP和AH定义了协议和载荷头的格式及所提供的服务，但却没有定义实现以上能力所需具体转码方式，转码方式包括对数据转换方式，如算法、密钥长度等。为简化IPSec的使用和管理，IPSec还可以通过IKE进行自动协商交换密钥、建立和维护安全联盟的服务。具体介绍如下：

AH协议：AH是报文头验证协议，主要提供的功能有数据源验证、数据完整性校验和防报文重放功能。然而，AH并不加密所保护的数据报。

ESP协议：ESP是封装安全载荷协议。它除提供AH协议的所有功能外（但其数据完整性校验不包括IP头），还可提供对IP报文的加密功能。

IKE协议：IKE协议用于自动协商AH和ESP所使用的密码算法。

## IPSec VPN的特点

- IPSec (Internet 协议安全)是一个工业标准网络安全协议，为 IP 网络通信提供透明的安全服务。IPSec可以提供：
  - 访问控制
  - 无连接的完整性、数据来源验证
  - 防重放
  - 机密性（加密）

**在IP层对数据保护**

- 对于上层应用是透明；
- 对于底层通信没有任何特殊要求。



**基于策略的安全保护**

- 定义安全保护的粒度；
- 可以灵活的制订策略满足复杂的安全需求。








IPSec (Internet 协议安全)是一个工业标准网络安全协议，为 IP 网络通信提供透明的安全服务，保护 TCP/IP 通信免遭窃听和篡改，可以有效抵御网络攻击，同时保持易用性。IPSec可以提供：

- **访问控制**

通信对等体认证机制，对于通信的对等体进行认证，从而完成访问控制功能。

- **无连接的完整性、数据来源验证**

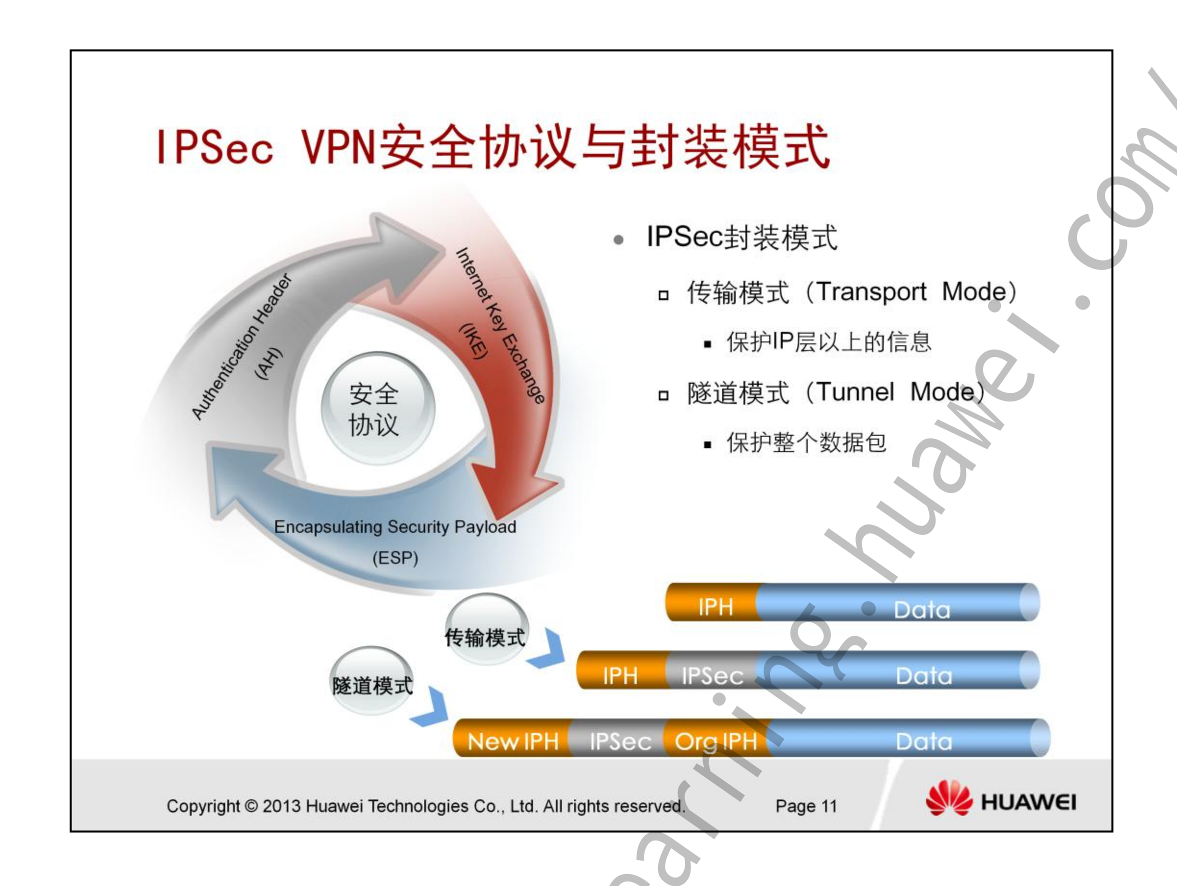
通过报文认证，防止传输过程中数据被篡改，确保发出数据和接收数据的一致性。IPSec利用Hash函数为每个数据包产生一个加密校验和，接收方在打开包前先计算校验和，若包遭篡改导致校验和不相符，数据包即被丢弃。

- **防重放**

通过AH或者ESP的防重放窗口结合认证，来抵御重放攻击。确保每个IP包的唯一性，保证信息万一被截取复制后，不能再被重新利用、重新传输回目的地址。该特性可以防止攻击者截取破译信息后，再用相同的信息包冒取非法访问权（即使这种冒取行为发生在数月之后）。

- **机密性（加密）**

通过ESP的加密功能以及ESP协议的报文填充功能来完成。在传输前，对数据进行加密，可以保证在传输过程中，即使数据包遭截取，信息也无法被读出。该特性在IPSec中为可选项，与IPSec策略的具体设置相关。



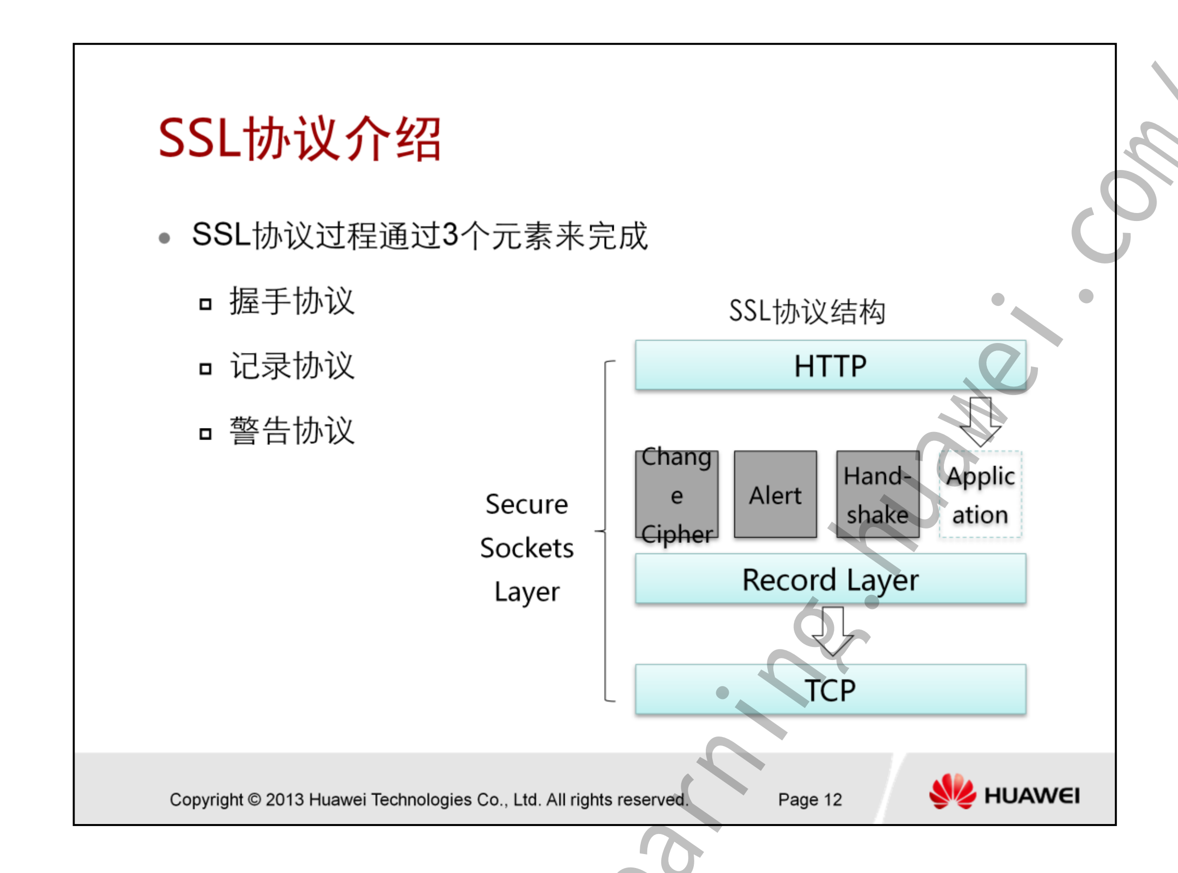

**AH协议:**

AH报头插在IP报头之后，TCP、UDP或者ICMP等上层协议报头之前。一般AH为整个数据包提供完整性检查，但如果IP报头中包含“生存期（Time To Live）”或“服务类型（Type of Service）”等值可变字段，则在进行完整性检查时应将这些值可变字段去除。

AH也为IP头中的一部分提供验证，在某些情况下，这可能是必须的。例如，如果IPv4选项或IPv6扩展头的完整性在发送方和接收方之间的路程中必须被保护，AH可以提供这项服务（除了IP头中不可预知、易变的部分）。

在使用AH协议时，AH协议首先在原数据前生成一个AH报文头，报文头中包括一个递增的序列号（Sequence number）与验证字段（空）、安全参数索引（SPI）等。AH协议将对新的数据包进行离散运算，生成一个验证字段（authentication data），填入AH头的验证字段。AH协议目前提供了两种散列算法可选择，分别是：MD5和SHA1，这两种算法的密钥长度分别是128bit和160bit。

AH协议使用32比特序列号结合防重放窗口(一般为64位)和报文验证来防御重放攻击。当收到了一个经过认证的数据以后，防重放窗口会滑动一次，如果该数据被重放，由于其顺序号码和原来的相同，因此这个数据会落到窗口之外，数据就会被丢弃。




握手协议：

这个协议负责配置用于客户机和服务器之间会话的加密参数。当一个SSL客户机和服务器第一次开始通信时，它们在一个协议版本上达成一致，选择加密算法和认证方式，并使用公钥来生成共享密钥。

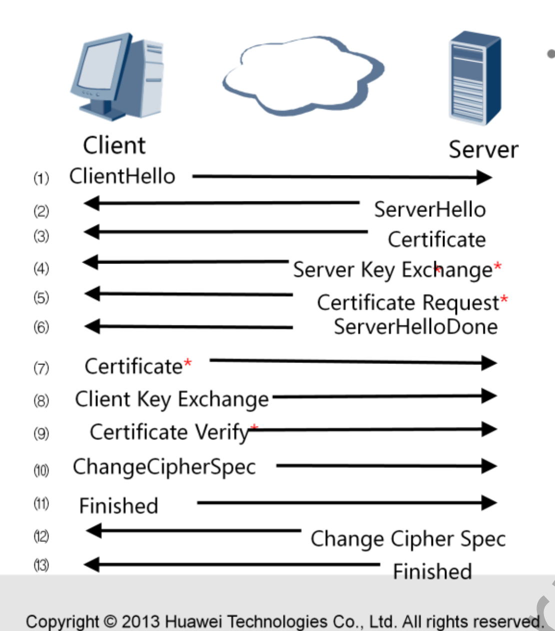
记录协议：

这个协议用于交换应用数据。应用程序消息被分割成可管理的数据块，还可以压缩，并产生一个MAC（消息认证代码），然后结果被加密并传输。接收方接收数据并对它解密，校验MAC，解压并重新组合，把结果提供给应用程序协议。

警告协议：

这个协议用于表示在什么时候发生了错误或两个主机之间的会话在什么时候终止。

# SSL原理—握手协议




- 在用SSL进行通信之前，首先要使用SSL的HandShake协议在通信两端握手，协商数据传输中要用到的相关安全参数（如加密算法、共享密钥、产生密钥所要的材料等），并对对端的身份进行验证。









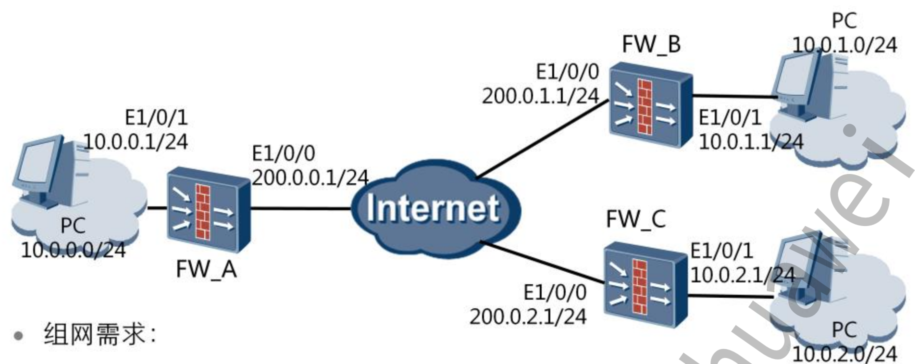
# 目录








# 建立点到多点SA策略模板(1)+子策略方式(2)




- 组网需求：
  - FWA、FWB公网IP是固定公网地址，FWC公网地址为动态获取；
  - FWA与FWC之间需要使用野蛮模式，且只能由FWC主动发起连接；
  - FWA与FWB之间可以使用主模式/野蛮模式，两边都可以主动发起连接；
  - 使用pre-shared key验证方法的提议配置验证字；
  - 使用策略模版+子策略方式。








防火墙上必须有到达对方私网网段的正确路由(尽管该路由可能是不可达的,可以是明细路由,可以是默认路由等)，此条路由的出接口一定是使能IPSEC policy的接口，该路由的作用是将需要IPSEC加密的报文送到使能IPSEC policy的接口进行处理。

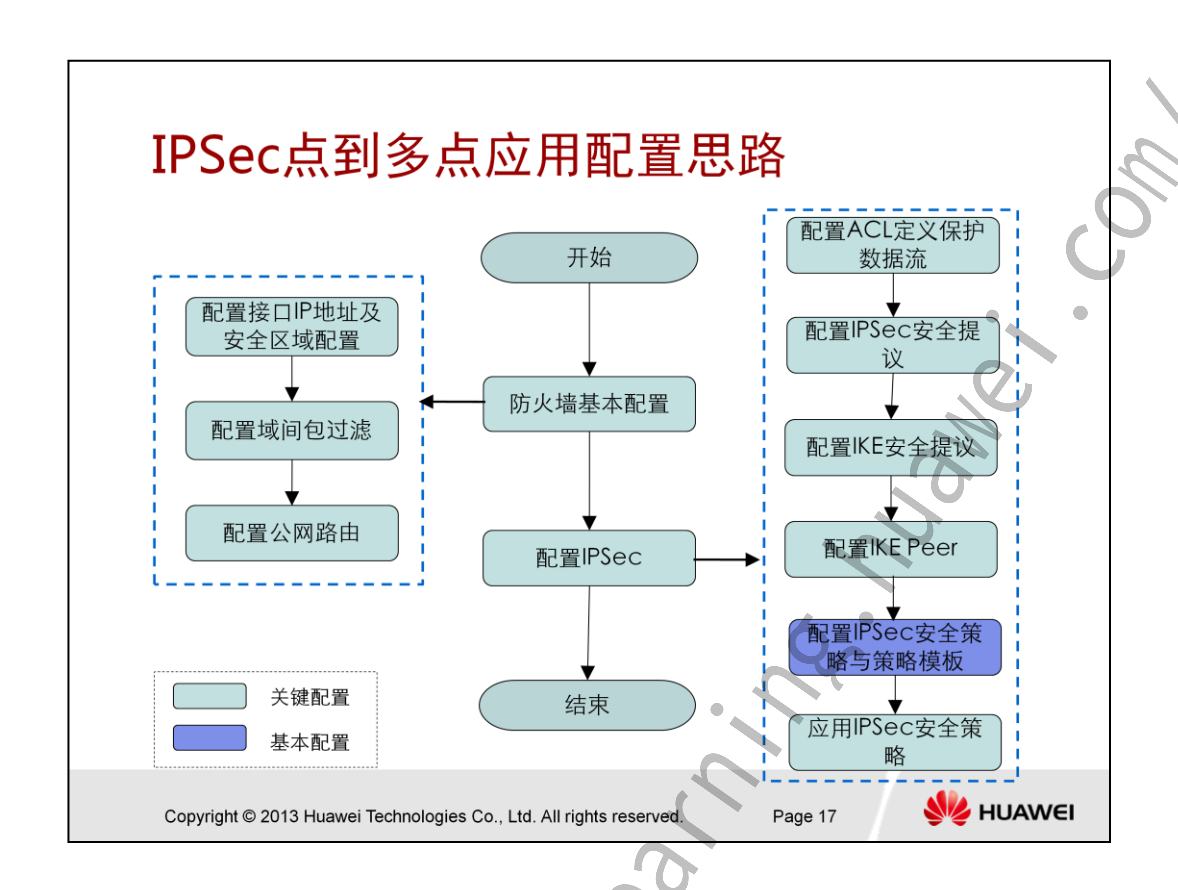
USG50/2100/2200/3000连接内网的接口需要取消接口快转功能,否则IPSEC SA不会触发建立,命令为undo ip fast-forwarding qff, 出接口无需配置该命令。

注意总部和分支节点的ACL配置，主动触发IPSEC VPN防火墙(在策略模版方式下只能是分支机构防火墙)ACL中必须定义Source字段,一般推荐同时定义Source和Destination字段，如果ACL中只定义了destination字段,该防火墙不能主动触发IPSEC SA建立,但可以被动响应对端的IPSEC SA请求,建立IPSEC SA。策略模版+子策略是指在安全策略的某个子策略中使用策略模版方式,其他子策略不一定使用策略模版.即:

ipsec policy map1 10 isakmp

ipsec policy map1 20 isakmp template map1tmp

只要是使用了策略模版,都不能作为IPSEC SA的发起方。在总部防火墙上配置多个IKE peer，一个静态节点对应一个peer，所有动态节点对应一个peer，该IKE peer不需要指定remote-address,因为其他分支机构的公网IP不固定。同一个IPSec安全策略组中模板方式安全策略的序号必须大于直接创建的安全策略的序号。即同一个IPSec安全策略组中模板方式安全策略的优先级必须最低，否则可能导致协商失败。




在配置IPSec安全策略与策略模板时，USG_A上配置一条模板方式的安全策略，一条IKE安全策略直接创建的IPSec安全策略。USG_B、USG_C配置IKE安全策略直接创建的IPSec安全策略。

# FWA关键配置-1

- 配置IKE Peer

  # 创建名为a的IKE peer，为每一个静态分支创建一个Peer

  [FWA] ike peer a

  [FWA-ike-peer-a] remote-address 200.0.1.1

  [FWA] ike peer a'

  [FWA-ike-peer-a'] exchange-mode aggressive








FWB配置注意事项：

- FWB的ACL与FWA的ACL3000成相互映射。
- IKE peer中的remote-address参数应设置为FWA的公网地址。
- IKE peer应与FWA的IKE peer a对应。

# FWA关键配置-2

- 配置安全子策略和策略模版

  # 创建安全策略map1的子策略10，引用ike-peer a。

  [FWA] ipsec policy map1 10 isakmp

  [FWA-ipsec-policy-isakmp-map1-10] ike-peer a

  # 创建安全策略模版map1tmp，# 引用ike-peer a’。

  [FWA] ipsec policy-template map1tmp 10

  [FWA-ipsec-policy-templet-map1tmp-10] ike-peer a'

  # 创建安全策略map1的子策略20, 引用策略模版map1tmp

  [FWA] ipsec policy map1 20 isakmp template map1tmp

- 配置防火墙C时，配置IKE的协商模式为野蛮模式

  [FWC] ike peer c

  [FWC-ike-peer-c] exchange-mode aggressive







- **配置安全子策略和策略模版**

  # 创建安全策略map1的子策略10。

  [FWA] ipsec policy map1 10 isakmp

  [FWA-ipsec-policy-isakmp-map1-10] ike-peer a

  [FWA-ipsec-policy-isakmp-map1-10] proposal tran1

  [FWA-ipsec-policy-isakmp-map1-10] security acl 3000

  [FWA-ipsec-policy-isakmp-map1-10] quit

  # 创建安全策略模版map1tmp。

  [FWA] ipsec policy-template map1tmp 10

  [FWA-ipsec-policy-templet-map1tmp-10] ike-peer a'

  [FWA-ipsec-policy-templet-map1tmp-10] proposal tran1

  [FWA-ipsec-policy-templet-map1tmp-10] security acl 3001

  # 创建安全策略map1的子策略20, 引用策略模版map1tmp

  [FWA] ipsec policy map1 20 isakmp template map1tmp

- **引用安全策略**

  [FWA] interface Ethernet 1/0/0



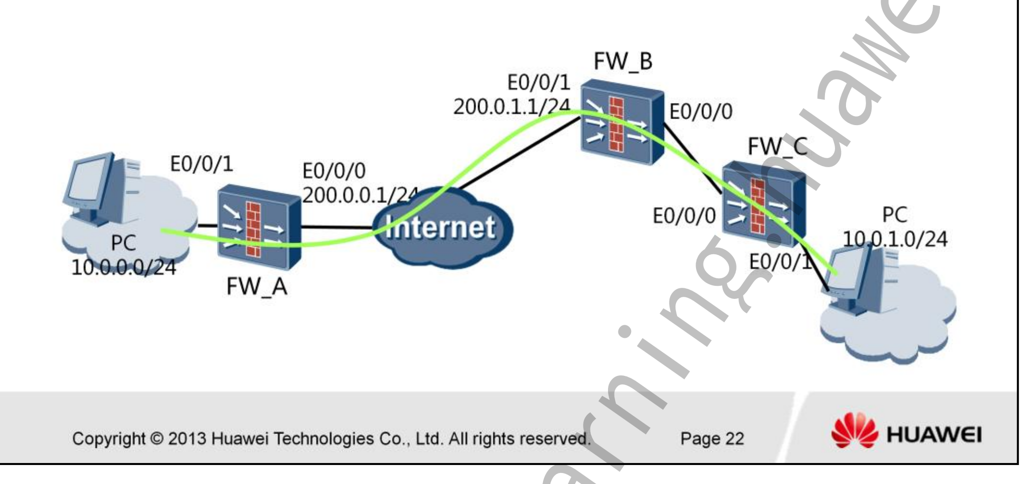
# 目录












私网用户在通过internet访问远端网络时，私网地址将通过NAT设备进行转换。在IPSec点到点的应用场景中，会对IP包头或端口信息进行验证，由于NAT网关将原IP地址或端口信息进行了转换，因此影响IPSec的验证及信息传递。

## IPSec NAT穿越分析

- AH无法穿越NAT
  - AH对整个报文进行认证
- ESP穿越NAT的问题
  - ESP会加密报文的端口信息
- 主模式和野蛮模式如何穿越NAT
  - NAT导致IP地址变化影响IP+预共享密钥的验证

推荐配置　Name验证方式+pre-sharekey+子策略/策略模板





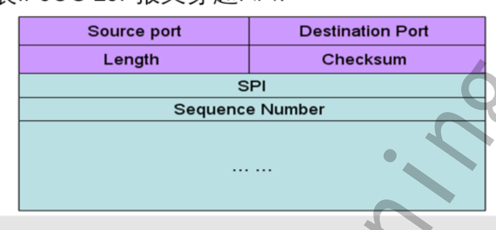

AH无法穿越NAT，由于AH对整个IP都进行验证，NAT网关会改变IP头的地址，造成AH验证失败。而ESP只对IP负载进行验证，因而可以解决这个问题。

ESP会将第四层的端口信息加密而造成PAT问题。采用IPSec透明NAT功能可以解决这个问题，将ESP分组封装在UDP头中并且附带必需的端口信息以使PAT正常工作。

IPSec NAT穿越不支持IKE主模式、野蛮模式的IP地址+预共享密钥方式验证，因为预共享密钥方式验证需要在IP报文中提取源IP地址从而查找这个地址对应的预共享密钥(前面已经介绍过)，而由于NAT的存在造成了地址变化使设备无法查找预共享密钥。如果NAT穿越需要使用主模式，可以采用证书验证的方法解决；如果NAT穿越需要使用野蛮模式，可以采用Name方式验证。

## IPSec NAT穿越原理

- NAT穿越能力协商
  - 在第一阶段IKE协商中通过VenderID进行能力协商。
- NAT网关检测
  - 在第一阶段IKE协商中使用NAT-D负载用于发现是否存在NAT。
- NAT穿越功能启用协商
  - IKE第二阶段的SA载荷中协商是否使用NAT穿越。
- 使用UDP封装IPSec ESP报文穿越NAT






HUAWEI

NAT穿越能力由IKE消息携带的厂商ID来决定。

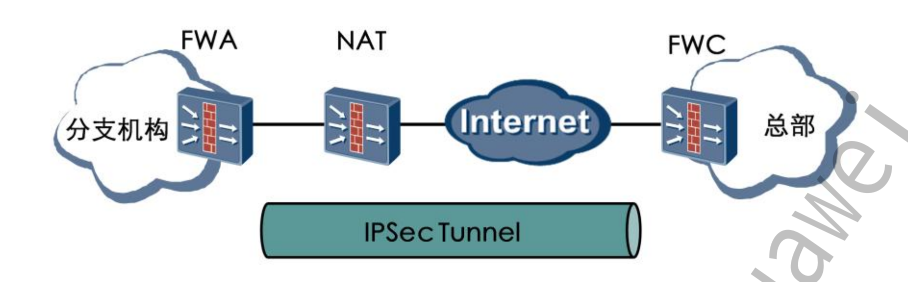
为了侦测IP地址或者端口信息是否在传输过程中发生变化，双方交换IP地址/端口号的hash值，Hash值不同，说明使用了NAT或者PAT。Hash值以NAT-D负载进行发送，一个NAT-D负载包含一个Hash值，一般情况下，只有本端和对端的两个Hash值。NAT-D负载包含在主模式的消息3、4中或者是包含在野蛮模式的消息2、3中。

当设备检测到有NAT存在时，发起方将消息5、6的源端口和目的端口都设置为4500，所有和发起方交换的IKE消息都使用4500端口通信，如果发起方在NAT内部，则NAT将发起方的源端口改为其他端口和其他设备通信。

IKE第一阶段完成后，通信双方都知道了NAT的存在，然后在IKE第二阶段的SA载荷中协商是否使用NAT穿越，通过增加两个新的封装模式来进行：UDP-隧道模式、UDP-传输模式。

在UDP报头后面直接封装了一个ESP报文头。在UDP报文头中源端口号以及目的端口号采用和IKE协议一致的端口号。这样可以减少NAT网关上NAT会话的数量，并且在配置和使用都非常简单。但是共用端口号的同时带的另一个问题是上层实现如何区分一个报文是IKE报文还是UDP封装的ESP报文呢？为了区分这两种报文，RFC3948规定采用UDP封装方式的ESP报文的SPI一定不能为0，同时规定使用启用NAT穿越的IKE协商报文在UDP报文头后插入4个值为0的字节，作为非ESP报文的标识。

## IPSec NAT穿越典型场景




- 场景分析
  - FWA与FWC之间需要建立IPSec隧道；
  - FWA通过分支机构宽带接入公网，即FWA外网口获得的是一私网地址；
  - NAT设备将分支机构的用户私有地址转换为公网地址以便在公网路由。







**FWA关键配置：**

# 配置IKE本地名称。

[USG5000A] ike local-name USG5000A

# 配置IKE peer。

[USG5000A] ike peer b

[USG5000A-ike-peer-b] undo version 2

[USG5000A-ike-peer-b] exchange-mode aggressive

[USG5000A-ike-peer-b] local-id-type name

[USG5000A-ike-peer-b] remote-name USG5000C

[USG5000A-ike-peer-b] ike-proposal 10

[USG5000A-ike-peer-b] remote-address 131.108.5.2

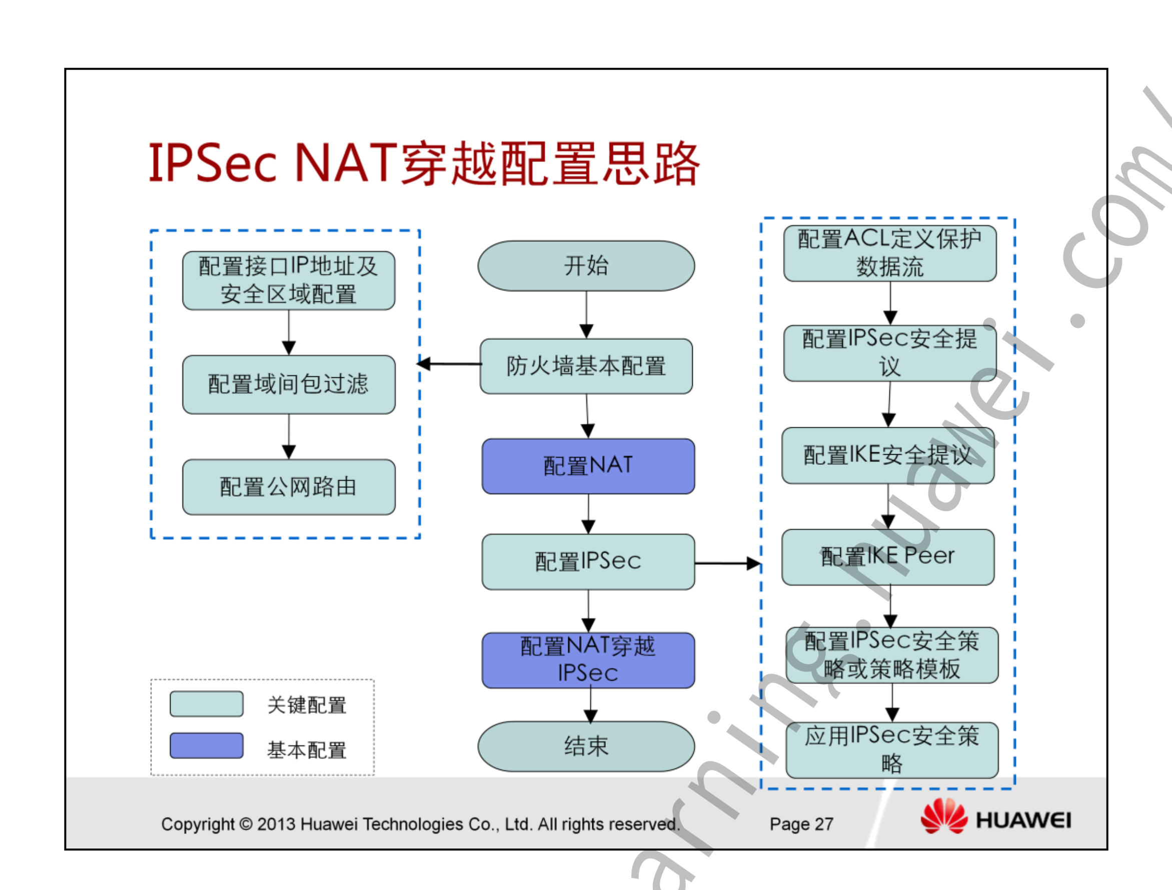
[USG5000A-ike-peer-b] pre-shared-key abcde

[USG5000A-ike-peer-b] nat traversal

[USG5000A-ike-peer-b] quit

# 配置采用IKE方式协商IPSec安全策略map1。

[USG5000A] ipsec policy map1 10 isakmp


IPSec NAT穿越配置思路
配置接口IP地址及安全区域配置
配置域间包过滤
配置公网路由
开始
防火墙基本配置
配置NAT
配置IPSec
配置NAT穿越IPSec
结束
配置ACL定义保护数据流
配置IPSec安全提议
配置IKE安全提议
配置IKE Peer
配置IPSec安全策略或策略模板
应用IPSec安全策略
关键配置
基本配置
Page 27
HUAWEI

# 关键配置



[FWA-ike-peer-a]nat traversal

- IPSec NAT穿越功能配置比较简单，和普通IPSec VPN的配置最大的区别就在于多了这条命令；
- 认证方式需要使用pre-sharekey+Name认证方式；
- FWB的配置、型号与IPSec隧道的建立无关。只需保证FWC经过FWB做地址转换后还可和FWA互通。
- IPSec隧道两端均需配置该命令。








**FWC关键配置：**

# 配置IKE 本地名称。

[USG5000C] ike local-name USG5000C

# 配置IKE peer。

[USG5000C] ike peer a

[USG5000C-ike-peer-a] undo version 2

[USG5000C-ike-peer-a] exchange-mode aggressive

[USG5000C-ike-peer-a] local-id-type name

[USG5000C-ike-peer-a] remote-name USG5000A

[USG5000C-ike-peer-a] ike-proposal 10

[USG5000C-ike-peer-a] remote-address 131.108.5.100 131.108.5.110

[USG5000C-ike-peer-a] pre-shared-key abcde

[USG5000C-ike-peer-a] nat traversal

[USG5000C-ike-peer-a] quit

# 配置采用IKE策略模板方式协商IPSec安全策略模板map_temp。

[USG5000C] ipsec policy-template map_temp 1

## IPSec NAT穿越WEB配置

VPN > IPSec > IKE协商

对端网关VPN实例 public
对端网关IP 131.108.5.2
对端地址池范围
VPN实例 public
高级
加密算法 DES-CBC 认证算法 SHA1
DH组 DH-Group1
完整性算法 HMAC-SHA1
SA超时时间 86400 *<60-604800>秒
DPD工作模式 ----- NONE -----
NAT穿越 启动
对端认证IP地址
应用 返回

启用NAT穿越功能

  HUAWEI

使用Web配置方式配置IPSec NAT穿越情况时，需要在配置IKE协商阶段一时启用NAT穿越功能。

选择“VPN > IPSec > IKE协商”。在“IKE协商列表”中，单击“阶段1”。 在高级配置中，勾选NAT穿越功能。

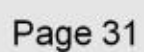


# 目录

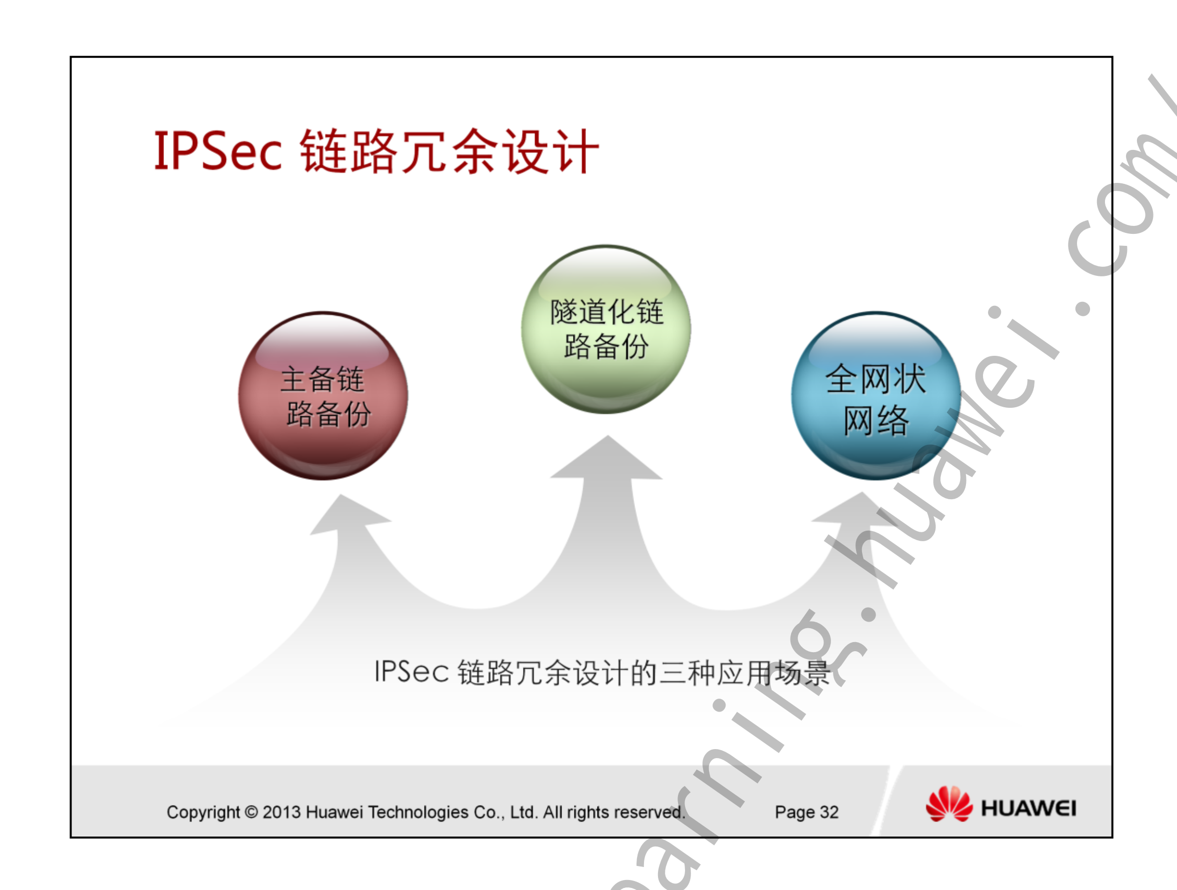













- 主备链路备份

一般情况下，主用IPSec隧道采用以太网链路固定IP接入，备用IPSec隧道采用以太网链路或拨号链路（PPPoE/ADSL/3G）接入均可。主用链路故障时业务倒换到备用链路。

- 隧道化链路备份

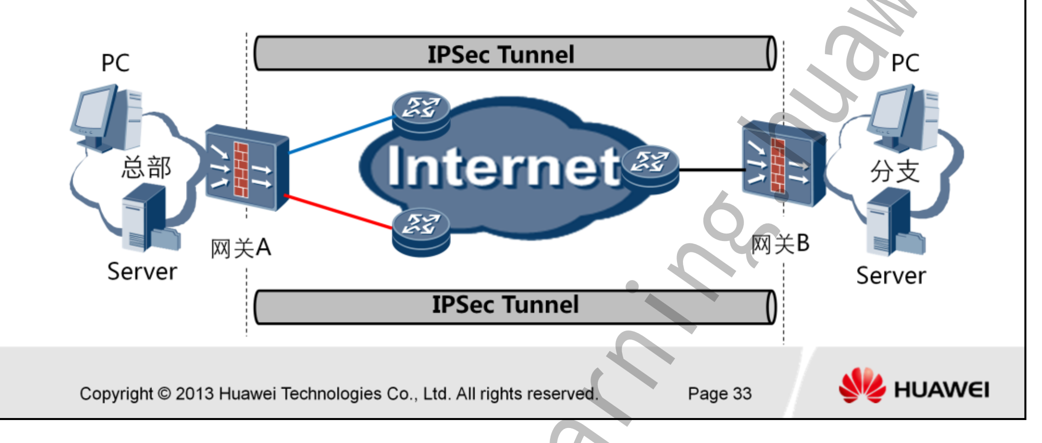
将IPSec策略应用到Tunnel接口上，IPSec策略跟具体的物理接口没有绑定关系，从而实现出接口链路的备份。当一条链路出现问题时，可直接路由到其他链路传输。

- 全网状网络:

每个设备都与其它设备之间建立IPSec隧道，这是最为安全的网络结构，但需要较多的资金投入。

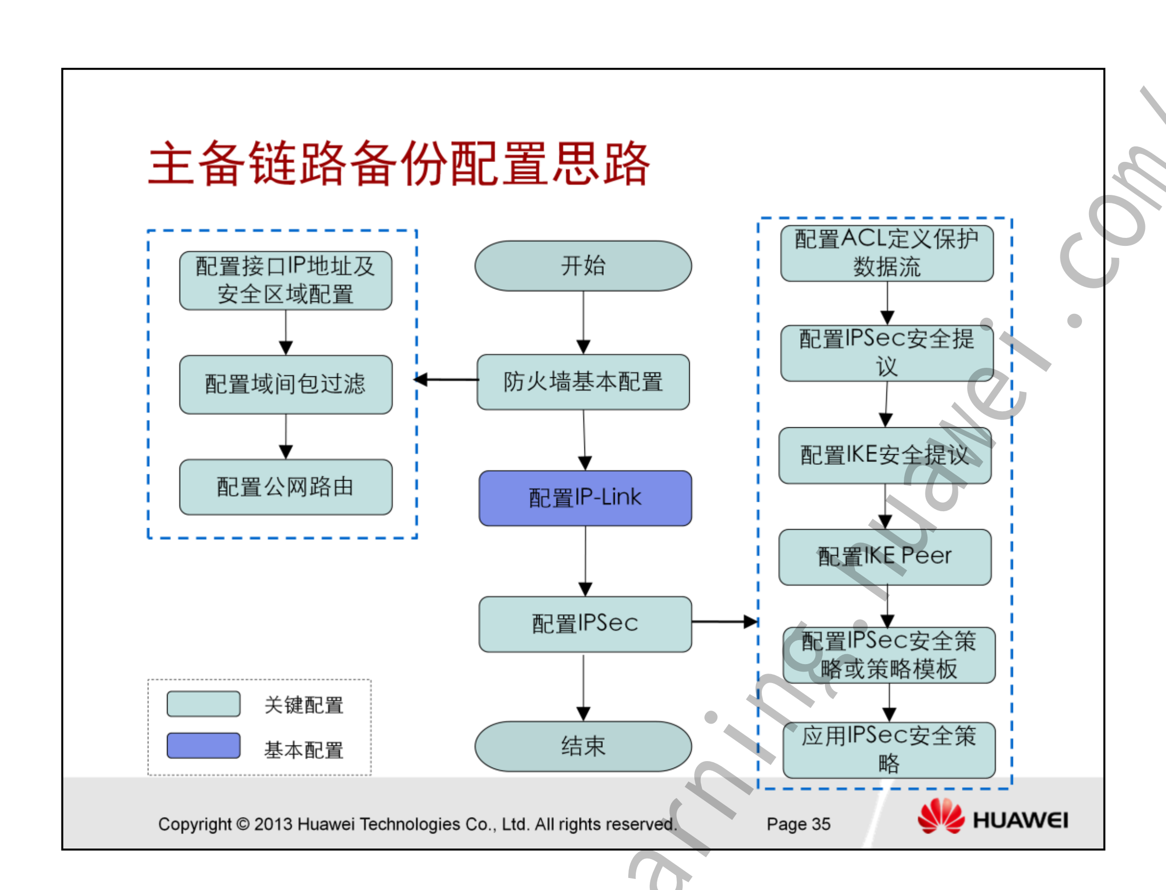
# IPSec链路冗余—主备链路备份

- 组网需求：
  - 网关A通过主备两条链路连接网关B。在网关A的两个物理接口分别应用IPSec策略，创建主备两条IPSec隧道。当主链路故障时，将在备份链路上建立新的IPSec隧道，并拆除旧的IPSec隧道，完成流量和隧道的切换。






备用IPSec隧道可采用的接入方式有PPPoE，ADSL，3G等。


主备链路备份配置思路
开始
防火墙基本配置
配置接口IP地址及安全区域配置
配置域间包过滤
配置公网路由
配置IP-Link
配置IPSec
结束
配置ACL定义保护数据流
配置IPSec安全提议
配置IKE安全提议
配置IKE Peer
配置IPSec安全策略或策略模板
应用IPSec安全策略
关键配置
基本配置
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 35
HUAWEI

# 主备链路备份关键配置

- 配置IP-link，分别检测到RT3的两个接口的链路状态

```
[USG] ip-link check enable
[USG] ip-link 1 destination 10.10.1.2 mode icmp
[USG] ip-link 2 destination 10.10.1.3 mode icmp
```

- 配置到达网关B的主备静态路由

```
[USG] ip route-static 0.0.0.0 0.0.0.0 10.10.1.2 track ip-link 1
[USG] ip route-static 0.0.0.0 0.0.0.0 10.10.1.3 preference 70 track ip-link 2
```



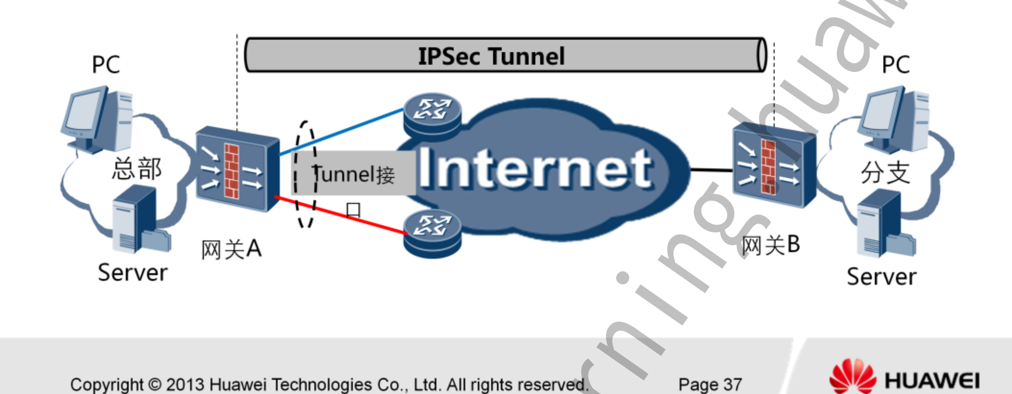





配置主链路的优先级高于备用链路。

# IPSec链路冗余--隧道化链路备份

- 组网需求：
  - 网关A通过主备两条链路连接网关B。在网关A的Tunnel接口和网关B的物理接口之间创建IPSec隧道，VPN流量通过Tunnel接口进行IPSec处理，然后通过路由表选择物理接口发送。



# 隧道化链路备份场景分析

- 在此种场景下，当主物理链路失效时，其路由变为不可达，流量自然切换到备用链路。这种情况下，IPSec隧道不需要进行重协商，故可快速完成流量切换。
- 将IPSec策略应用到Tunnel接口上，IPSec策略跟具体的物理接口没有绑定关系，从而实现出接口链路的备份。当一条链路出现问题时，可直接路由到其他链路传输。
- 在防火墙A上需创建tunnel接口并将接口加入相应安全区域，从防火墙A出口的IPSec流量需经过Tunnel接口选择合适的路由到达防火墙B。在防火墙B上也需要配置达到tunnel接口的静态路由。





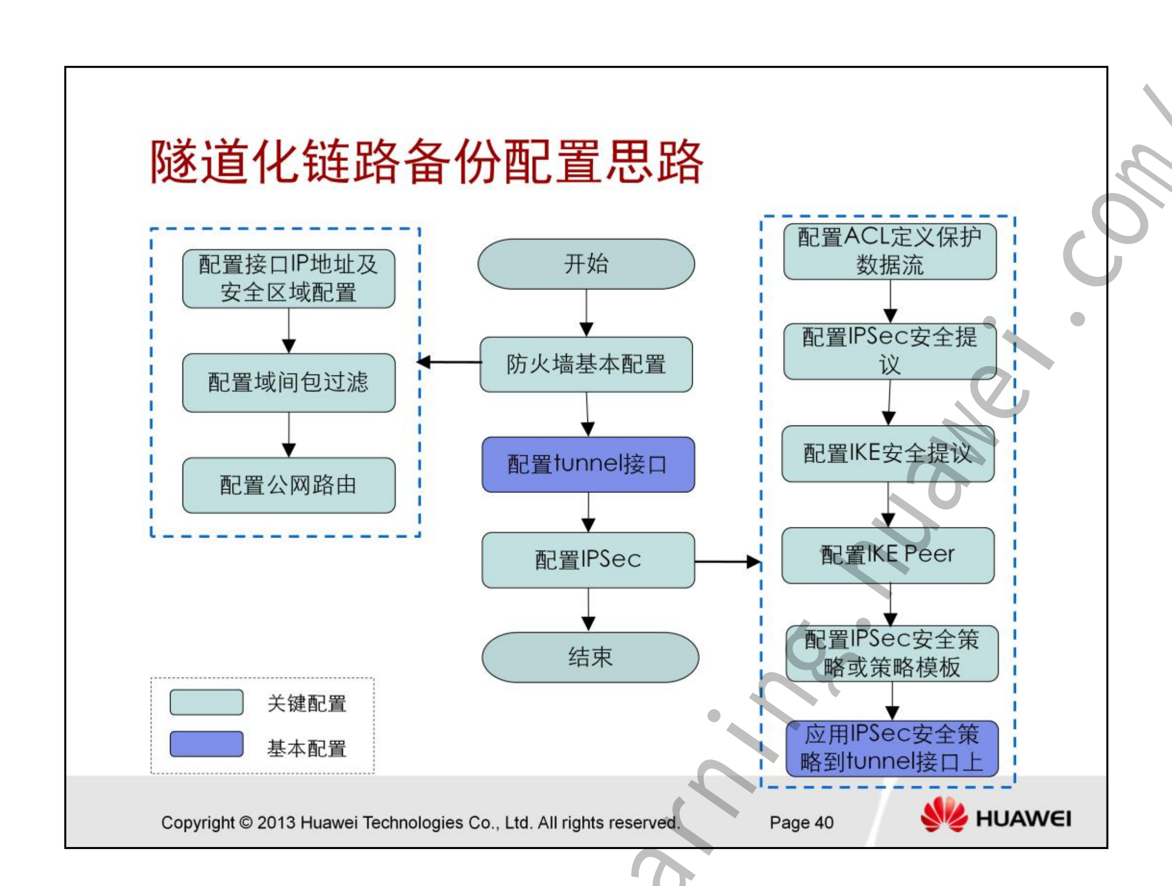




在此种场景下，当主物理链路失效时，其路由变为不可达，流量自然切换到备用链路。这种情况下，IPSec隧道不需要进行重协商，故可快速完成流量切换。

将IPSec策略应用到Tunnel接口上，IPSec策略跟具体的物理接口没有绑定关系，从而实现出接口链路的备份。当一条链路出现问题时，可直接路由到其他链路传输。

在防火墙A上需创建tunnel接口并将接口加入相应安全区域，从防火墙A出口的IPSec流量需经过Tunnel接口选择合适的路由到达防火墙B。在防火墙B上也需要配置达到tunnel接口的静态路由。



隧道化链路备份配置思路
开始
防火墙基本配置
配置tunnel接口
配置IPSec
结束
配置接口IP地址及安全区域配置
配置域间包过滤
配置公网路由
配置ACL定义保护数据流
配置IPSec安全提议
配置IKE安全提议
配置IKE Peer
配置IPSec安全策略或策略模板
应用IPSec安全策略到tunnel接口上
关键配置
基本配置
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 40
HUAWEI

# 隧道化链路备份关键配置

- 在网关A上配置Tunnel接口

  [USG_A] **interface tunnel 0**

  [USG_A-tunnel0] **tunnel-protocol ipsec**

  [USG_A-tunnel0] **ip address 1.1.1.2 24**

  [USG_A] **firewall zone trust**

  [USG_A-zone-trust] **add interface tunnel 0**

- 在网关A上将IPSec策略应用到tunnel接口上

  [USG_A] **interface tunnel 0**

  [USG_A-tunnel0] **ipsec policy  map1**








在防火墙A和B上的其余配置为IPSec标准配置。此处省略。



# 目录

1. VPN基础知识回顾
2. **IPSec VPN典型应用介绍**
   1. 点到多点IPSec VPN技术
   2. NAT穿越技术
   3. 链路冗余IPSec VPN应用场景
   4. **设备冗余IPsec VPN场景**
   5. 证书方式IPsec VPN场景
3. L2TP Over IPSec应用分析
4. SSL 应用分析

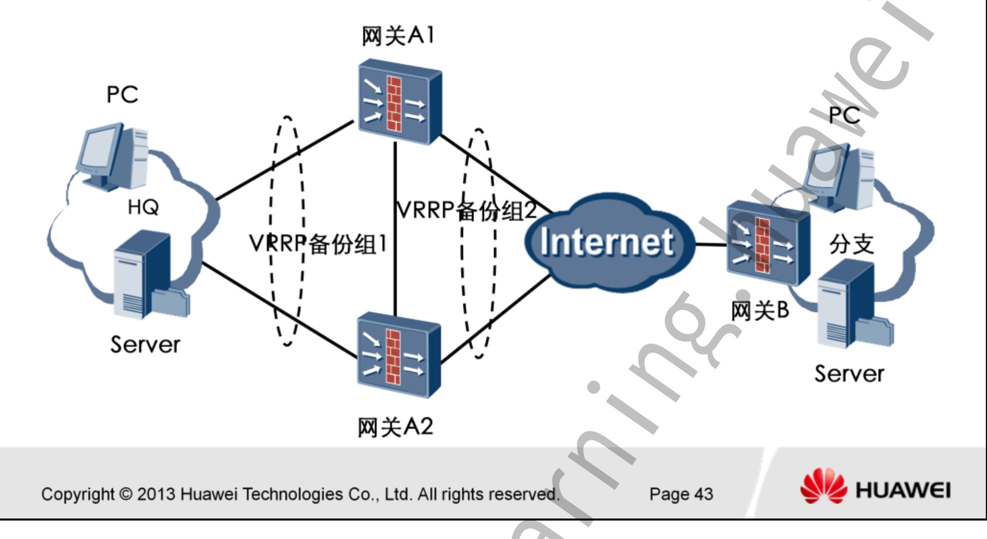






# IPSec 设备冗余设计

- IPSec VPN网关采用主备备份机制，当一台设备出现故障时，业务可以平滑的切换到备用设备上。



# IPSec双机热备场景分析

1

- 网关A1和A2为双机热备设备，A1为主设备A2为备用设备。

2

- 网关A1和A2对外配置虚拟接口1，并在虚拟接口1和分支网关B的物理接口之间建立IPSec隧道。

3

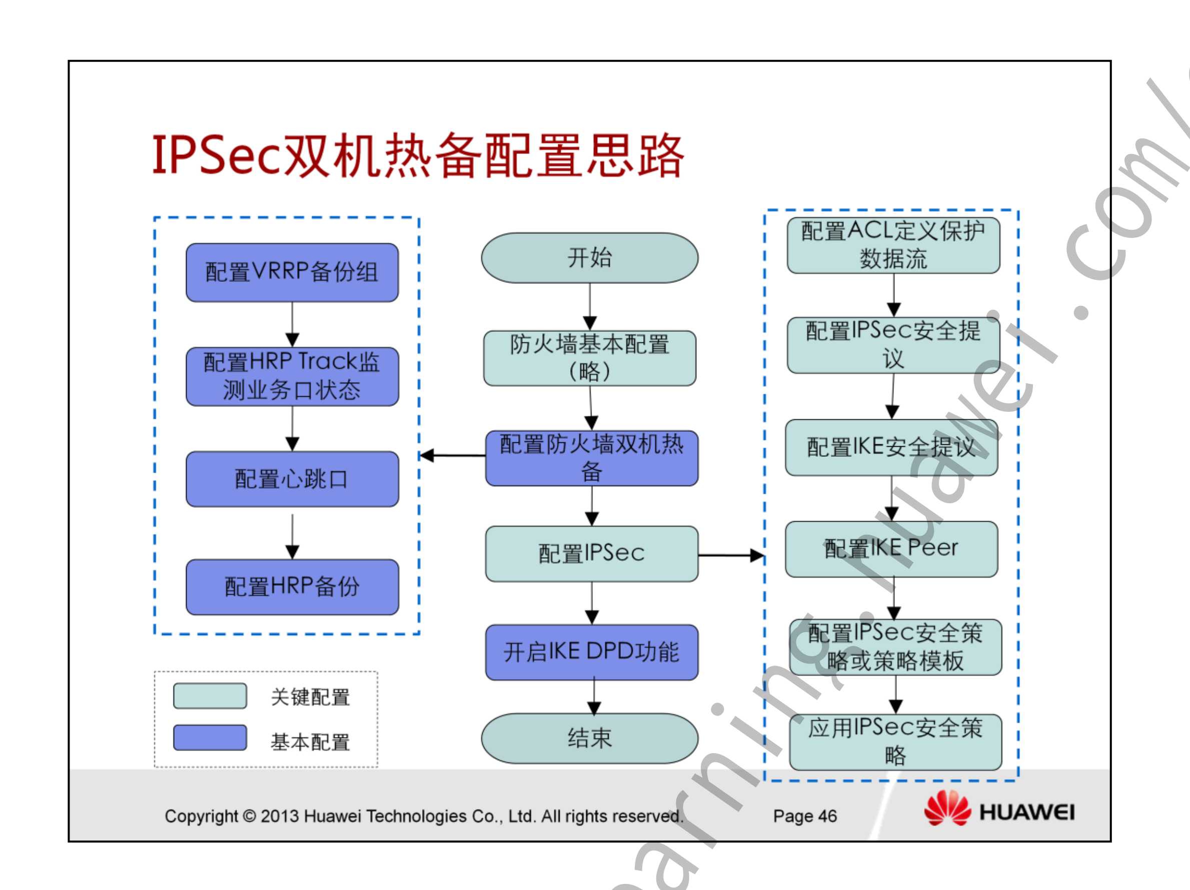
- 当主用网关A1物理接口、链路或主机故障时，流量被引导到备用网关A2进行IPSec和转发处理。这种情况下，原有的IPSec隧道并不会被拆除，切换速度更具优势。





# IPSec双机热备组网举例

USG_A
GE0/0/0
GE0/0/1
VRRP备份组1
10.100.10.2/24
VRRP备份组2
202.38.10.1/24
GE0/0/1
GE0/0/0
HQ
Internet
Branch
USG_C
Server
10.100.10.1/24
GE0/0/0
GE0/0/1
USG_B




主设备和隧道对端设备上都需开启IKE DPD功能。开启后，主备设备进行切换时，隧道对端设备（USG_C）能够快速感知，并与备用设备进行隧道协商。

如果主备防火墙本端使用非模板方式建立隧道，则务必要配置local address 为VRRP备份组2的IP地址，设置本端发起协商的地址为VRRP组的虚拟IP地址。

在配置防火墙C时，对端地址设置为VRRP组2的虚拟IP地址。

# IPSec双机热备配置（1）

- 防火墙基础配置。（接口IP地址及域间包过滤，略）
- 配置会话快速备份：

  [USG_A] **hrp mirror session enable**
- 配置HRP备份通道：

  [USG_A] **hrp interface GigabitEthernet 0/0/2**
- 配置抢占延时：

  [USG_A] **hrp preempt delay 300**
- 启动配置命令的自动备份功能：

  HRP_M[USG_A] **hrp auto-sync config**








配置VRRP备份组参考命令为：

[USG_A] **interface GigabitEthernet 0/0/1**

[USG_A-GigabitEthernet0/0/1] **vrrp vrid 1 virtual-ip 10.100.10.2 24 master**

[USG_A] **interface GigabitEthernet 0/0/3**

[USG_A-GigabitEthernet0/0/3] **vrrp vrid 2 virtual-ip 202.38.10.1 24 master**

此处配置的抢占延时是USG满配置时建议配置的抢占时间。根据实际配置的隧道数可以适当减小抢占时间的数值。

在防火墙上开启DPD功能，从而在总部网关发生主备切换时，能够快速感知，并与备用设备进行隧道协商。

## IPSec双机热备配置（2）

- IPSec相关配置

在配置防火墙C的IPSec时，对端地址设置为VRRP组的虚拟IP地址：

[USG_C] **ike peer peer1**

[USG_C-ike-peer-peer1] **remote-address 202.38.10.1**

在配置主备防火墙时，如果采用非策略模板形式，需配置本端IP地址为VRRP虚拟备份组IP地址：

[USG_A] **ipsec policy policy1 1 isakmp**

[USG_A-ipsec-policy-isakmp-policy1-1] **local-address 202.38.10.1**

在主设备和隧道对端设备上均需开启IKE DPD功能：

[USG_C] **ike dpd on-demand 10**








防火墙A上的IPSec配置按照标准步骤进行配置，防火墙A IPSec配置参考命令为：

HRP_M[USG_A] **acl 3003**

HRP_M[USG_A-acl-adv-3003] **rule permit ip source 10.100.10.0 0.0.0.255 destination 10.6.1.0 0.0.0.255**

HRP_M[USG_A-acl-adv-3003] **quit**

HRP_M[USG_A] **ipsec proposal pro1**

HRP_M[USG_A-ipsec-proposal-pro1] **quit**

HRP_M[USG_A] **ike proposal 1**

HRP_M[USG_A-ike-proposal-1] **quit**

HRP_M[USG_A] **ike peer peer1**

HRP_M[USG_A-ike-peer-peer1] **exchange-mode aggressive**

HRP_M[USG_A-ike-peer-peer1] **ike-proposal 1**

HRP_M[USG_A-ike-peer-peer1] **pre-shared-key security**

HRP_M[USG_A-ike-peer-peer1] **quit**

HRP_M[USG_A] **ike dpd on-demand 10**

HRP_M[USG_A] **ipsec policy-template temp1 1**

# IPSec双机热备配置（WEB）








HUAWEI



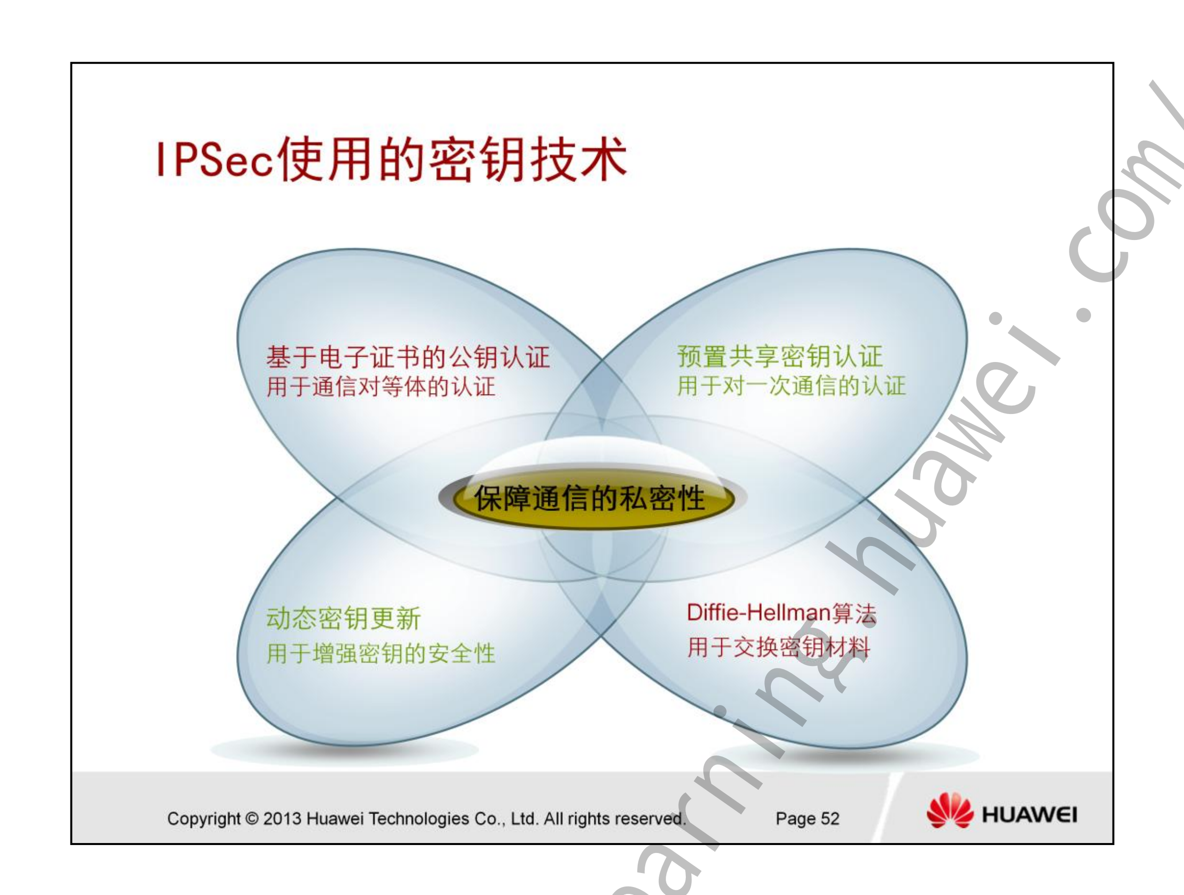
# 目录





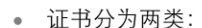







基于电子证书的公钥认证和预置共享密钥认证是可选的VPN隧道认证方法，动态密钥更新和D-H算法是建立隧道时用的密钥生成和管理方法。

## IPSec中的证书机制



- 证书机制可以为IPSec网络提供集中的密钥管理机制。在采用证书机制的IPSec网络中，每台设备都拥有CA颁发的证书，当设备之间进行通讯时，只要通过交换证书就可以确认对方的身份，并获得对方的公钥。这样当新设备加入时，只需要为新增加的设备申请一个证书，就可以与其他设备进行通讯，而不需要修改其他设备的配置。
- 证书分为两类:
  - CA证书
  - 本地（实体）证书




 Page 53




证书也称为数字证书，它建立了用户身份信息与用户公钥的关联。证书由第三方机构颁发，为通信双方提供身份验证功能。

证书是一段由CA（Certificate Authority）签名的包含用户身份信息、用户公钥信息以及身份验证机构数字签名的数据。CA对证书的签名保证了证书的合法性和权威性。目前证书的格式遵循ITU-T X.509 V3标准。

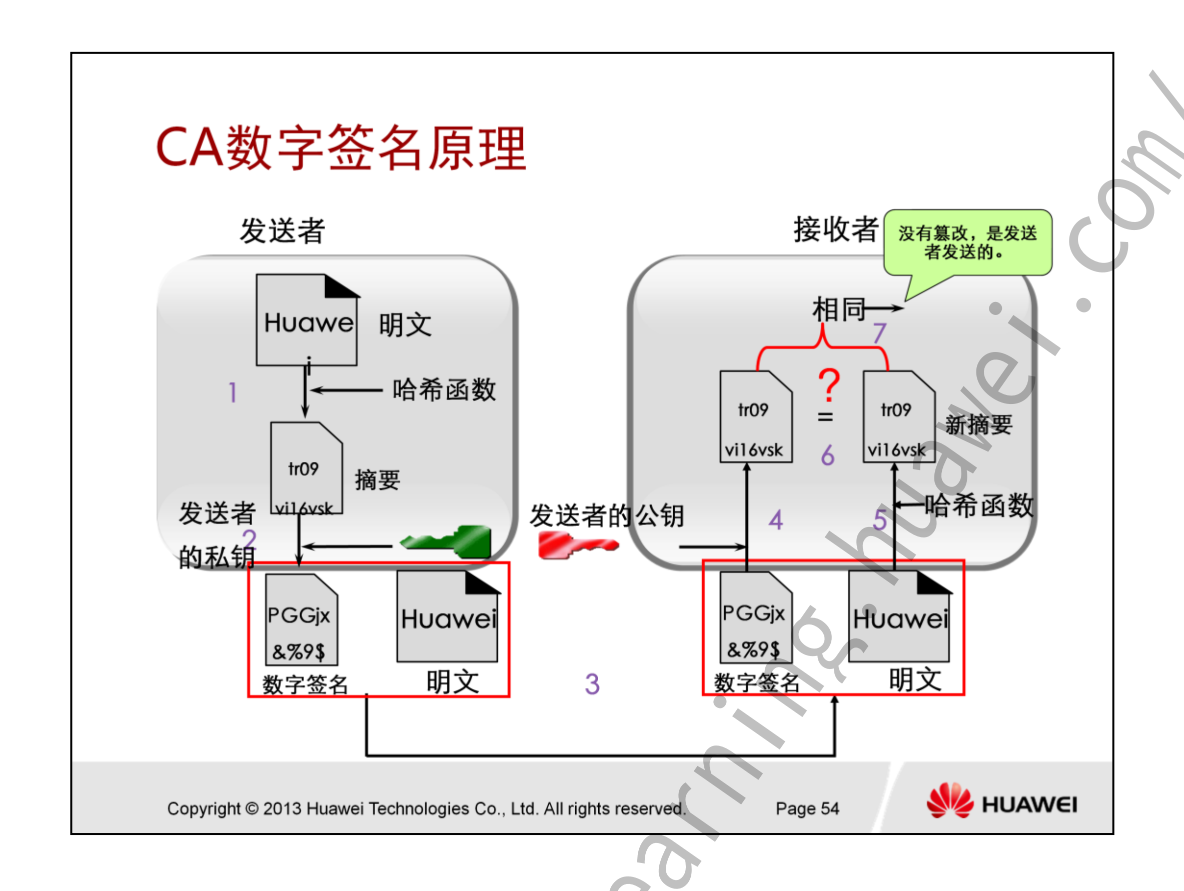
在USG9300上，证书可以用于通信双方建立IPSec隧道时的身份认证。在不采用证书机制的IPSec网络中，进行网络扩容时，每新增一台设备，都需要修改其余设备的配置。操作繁琐，且易出错。

- CA证书

颁发机构本身的证书，用于验证CA颁发的本地证书和证书吊销列表CRL（Certificate Revocation List）的有效性。

- 本地（实体）证书

由CA颁发，实体之间通信时使用。证书绑定了名字和本地公钥，如同网络身份证。




数字签名主要的功能是：保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。基于公钥密码体制和私钥密码体制都可以获得数字签名，目前主要是基于公钥密码体制的数字签名，包括普通数字签名和特殊数字签名。普通数字签名算法有RSA、ElGamal、Fiat-Shamir、Guillou-Quisquarter、Schnorr、Ong-Schnorr-Shamir数字签名算法、Des/DSA，椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等。数字签名技术是公钥密码体制的典型应用。数字签名的应用过程是，数据源发送方使用自己的私钥对数据校验和或其他与数据内容有关的变量进行加密处理，完成对数据的合法"签名"，数据接收方则利用对方的公钥来解读收到的"数字签名"，并将解读结果用于对数据完整性的检验，以确认签名的合法性。数字签名技术是在网络系统虚拟环境中确认身份的重要技术，完全可以代替现实过程中的"亲笔签字"，在技术和法律上有保证。在数字签名应用中，发送者的公钥可以很方便地得到，但他的私钥则需要严格保密。数字签名可用作数据完整性检查并提供拥有私钥的凭据，签署和验证数据的步骤如下

1. 发送者将一种散列算法应用于数据，并生成一个散列值；

2. 发送者使用私钥将散列值转换为数字签名；

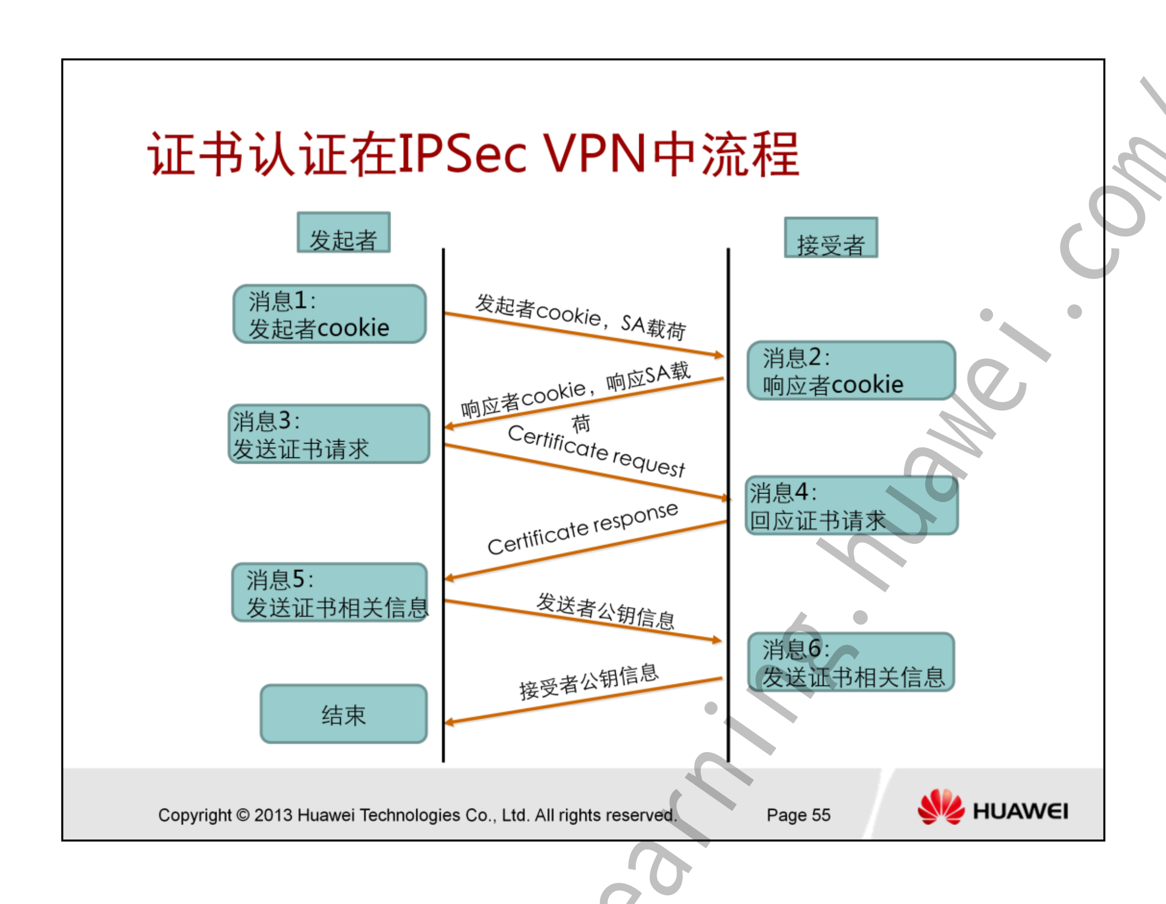
3. 发送者将数据、签名发给接收者；

4. 接收者使用发送者的公钥对数字前面进行解密；

5. 发送者将该散列算法应用于接收到的数据，并生成一个散列值；

6. 比较发送者发送的散列值与新生成的散列值是否相同。

7. 散列值相同则表示该消息来自与发送者，并且消息未被篡改。



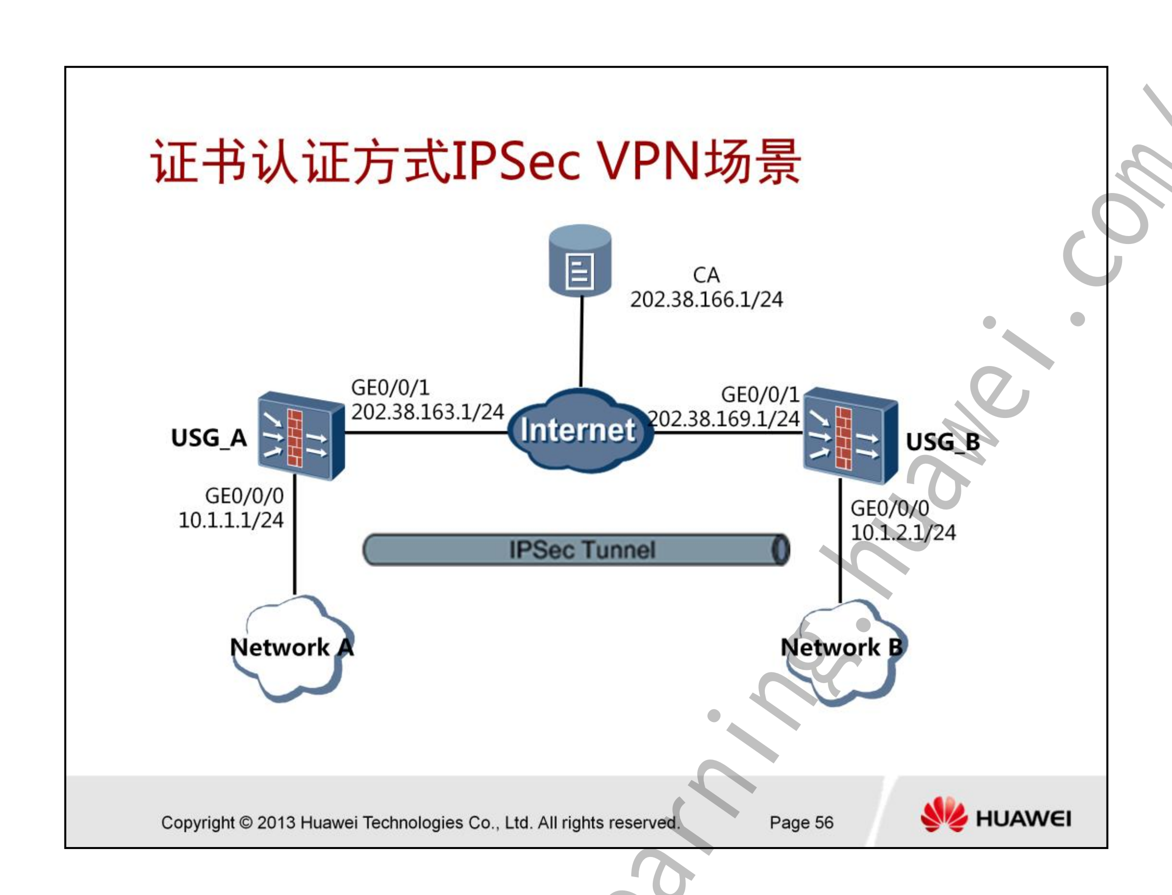

在IPSec IKE主模式协商的第一阶段中，将交换证书认证的相关信息。

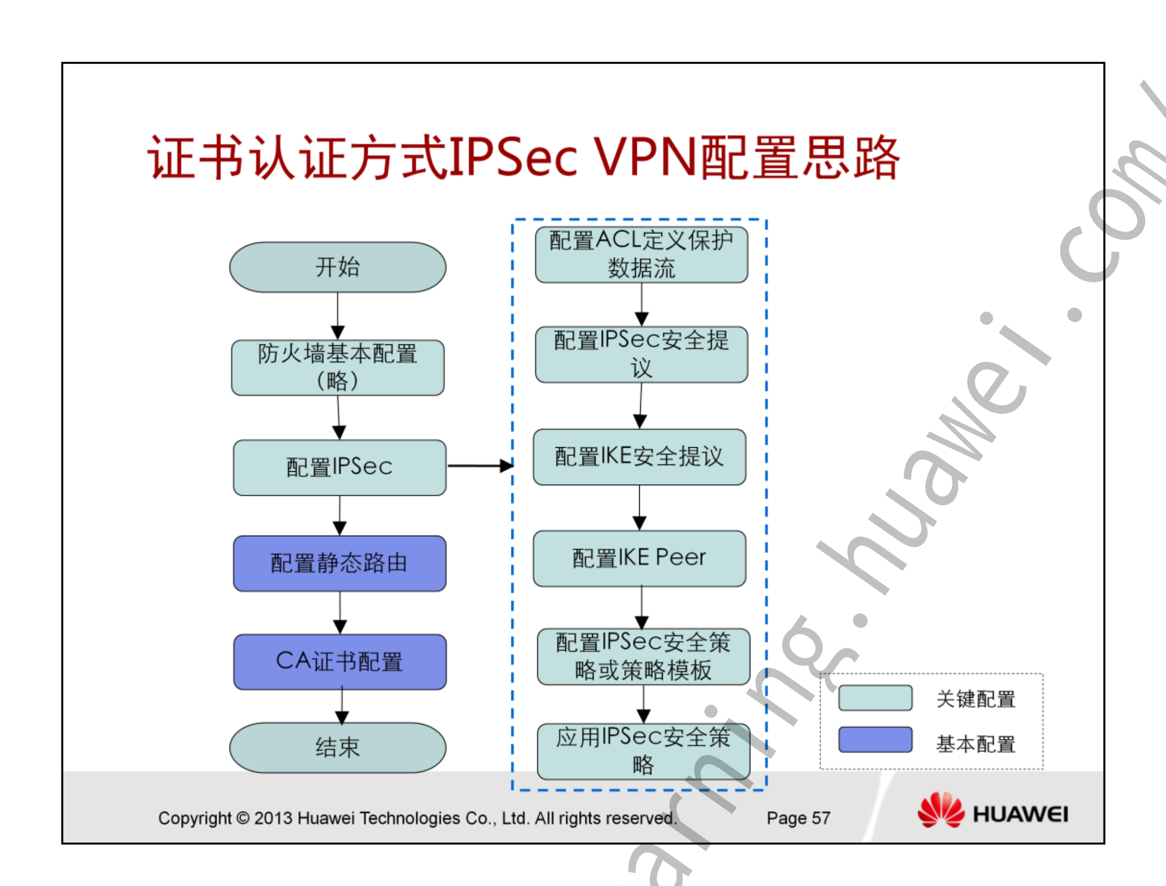
在消息3和消息4中，发送者发送证书请求，请求使用证书对身份进行认证；接受者收到请求后作出发送回应信息。

在消息5和消息6中，发送者和接受者相互相关数字签名所需要的公钥信息。并且对所交换的证书信息做验证。使用存储在本地的根证书的公钥来核实对方的实体证书签名，CA在给设备颁发实体证书时，会在实体证书后附加一个签名，我们可以通过根证书中的CA公钥来核实对方实体证书的签名。

如果通过了证书签名真实性验证，设备将当前时间和证书上的开始和终止时间做对比。如果设备时间在这两个值的范围内，有效期验证通过，否则，验证失败。

如果开启了CRL验证（依赖于设备的配置），设备将会在CRL中查找对方证书中的序列号，如果找到了序列号，则认为证书是无效的，验证失败；如果没有找到序列号，则证书验证通过。


证书认证方式IPSec VPN场景
CA
202.38.166.1/24
GE0/0/1
202.38.163.1/24
USG_A
Internet
GE0/0/1
202.38.169.1/24
USG_B
GE0/0/0
10.1.1.1/24
GE0/0/0
10.1.2.1/24
IPSec Tunnel
Network A
Network B
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 56
HUAWEI


证书认证方式IPSec VPN配置思路
开始
防火墙基本配置（略）
配置IPSec
配置静态路由
CA证书配置
结束
配置ACL定义保护数据流
配置IPSec安全提议
配置IKE安全提议
配置IKE Peer
配置IPSec安全策略或策略模板
应用IPSec安全策略
关键配置
基本配置
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 57
HUAWEI

## 关键配置 – 配置CA证书（1）

创建公私密钥对。

[USG_A] **rsa local-key-pair create**

配置PKI实体信息。

[USG_A] **pki entity entitya**

[USG_A-pki-entity-entitya] **common-name DeviceA**

[USG_A-pki-entity-entitya] **ip-address 202.38.163.1**

配置PKI域domaina。

[USG_A] **pki domain domaina** [

USG_A-domaina] **ca identifier ca_server1**

[USG_A-domaina] **certificate request entity entitya**

[USG_A-domaina] **certificate request url http://202.38.166.1:8889/certsrv/mscep/mscep.dll**








在防火墙A上，接口IP地址、安全区域及域间包过滤配置省略。

定义需要保护的数据流参考配置为：

[USG_A] **acl 3000**

[USG_A-acl-adv-3000] **rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255**

静态路由参考配置为：

[USG_A] **ip route-static 10.1.2.0 255.255.255.0 202.38.163.2**

当IPSec基于IP认证时，**ip-address**项为必配项，且该IP为和对端进行协商接口的IP。IPSec缺省为基于IP认证。

# 关键配置 – 配置CA证书（2）

在线申请CA证书和本地证书。

[USG_A] pki retrieval-certificate ca domain domaina

[USG_A] pki request-certificate domain domaina

- 导入本地证书和CA证书。假设在线获取到的本地证书为domaina_local.cer，CA证书为domaina_ca.cer。
- [USG_A] pki import-certificate local filename domaina_local.cer
- [USG_A] pki import-certificate ca filename domaina_ca.cer
- 开启CRL验证功能。

  [USG_A] pki crl check enable
- 配置自动更新CRL。

  [USG_A] **pki domain domaina**

  [USG_A-domaina] **crl auto-update enable**

  [USG_A-domaina] **crl update-period 3**







# 关键配置 – 配置IPSec

- 配置IPSec安全提议tran1，使用缺省配置。
  [USG9300A] ipsec proposal tran1
- 配置IKE安全提议，配置验证模式为rsa-sig，其余为使用缺省配置。
  [USG9300A] ike proposal 10
  [USG9300A-ike-proposal-10] authentication-method rsa-sig
- 配置IKE Peer。(略)
- 配置IPSec安全策略map1。（略）
- 在接口GigabitEthernet 1/0/2上应用安全策略map1。（略）





配置IKE Peer参考命令为：

[USG9300A] ike peer b
[USG9300A-ike-peer-b] ike-proposal 10
[USG9300A-ike-peer-b] certificate local-filename local.cer
[USG9300A-ike-peer-b] remote-address 202.38.169.1
[USG9300A-ike-peer-b] quit

配置IPSec安全策略map1参考命令为：

[USG9300A] ipsec policy map1 10 isakmp
[USG9300A-ipsec-policy-isakmp-map1-10] security acl 3000
[USG9300A-ipsec-policy-isakmp-map1-10] proposal tran1
[USG9300A-ipsec-policy-isakmp-map1-10] ike-peer b
[USG9300A-ipsec-policy-isakmp-map1-10] quit

在接口GigabitEthernet 1/0/2上应用安全策略map1参考命令为：

[USG9300A] interface GigabitEthernet 1/0/2
[USG9300A-GigabitEthernet1/0/2] ipsec policy map1



# 目录









# L2TP与IPSec功能对比

| | L2TP | IPSEC |
|---|---|---|
| 工作方式 | Client – Server | LAN-LAN,主机-主机 |
| OSI模型层次 | 二层 | 三层 |
| 多协议支持 | IP,IPX等 | IP |
| 安全机制 | 较弱的鉴别和加密 | 有完整内在安全机制 |
| 包认证 | NO | AH,ESP |
| 包加密 | NO | ESP |
| 密钥管理 | NO | ISAKMP |







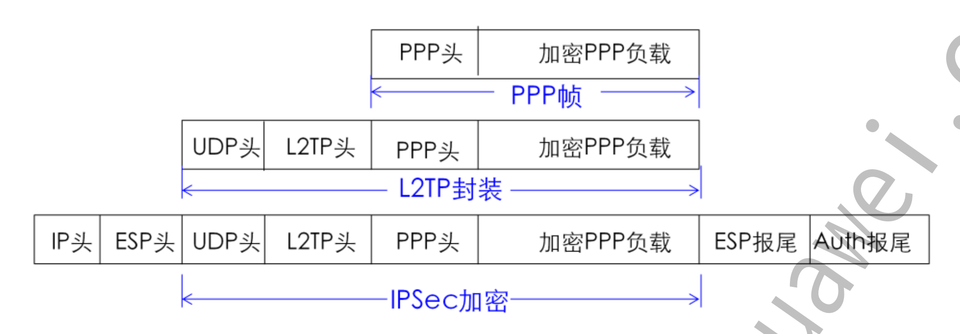


L2TP封装PPP分组的方式构建的，它利用L2TP协议在远程终端与企业内部网之间建立PPP会话通道，将远程终端连到企业内部网，同时利用PPP协议提供了支持多协议、多链路、数据压缩、PPP用户认证等功能 。

统的L2TP由于自身协议特点，存在安全隐患。配置L2TP over IPSec，即先用L2TP封装报文后再进行IPSec封装，可利用IPSec弥补L2TP的安全方面的不足，同时又利用L2TP弥补IPSec在用户认证、授权等方面的不足。

- **L2TP隧道存在以下安全隐患**
  - 攻击者可以通过窃取L2TP数据分组而知晓用户身份;
  - 攻击者可以修改L2TP控制数据和L2TP数据分组;
  - 攻击者可以劫持L2TP隧道或隧道中的PPP连接;
  - 攻击者可以终止PPP连接或L2TP隧道来进行DOS攻击;
  - 攻击者可以修改PPP ECP或CCP协议，以削弱或去除对PPP连接的机密性保护;也可通过破坏PPP LCP鉴别协议而削弱PPP鉴别过程的强度或获取用户口令。
- **制约IPSec协议构建远程访问型VPN的原因**
  - IPSec虽然提供了很强的主机级的身份鉴别，但它只能支持有限的用户级身份鉴别。而在远程访问型VPN中远程终端用户要进入企业内部网必须进行严格的身份鉴别。目前IPSec协议还不能方便、有效地实现这项功能;
  - 在IPSec安全协议中，总是假设封装分组是IP分组，目前尚不能支持多协议封装;

# L2TP over IPSec报文封装

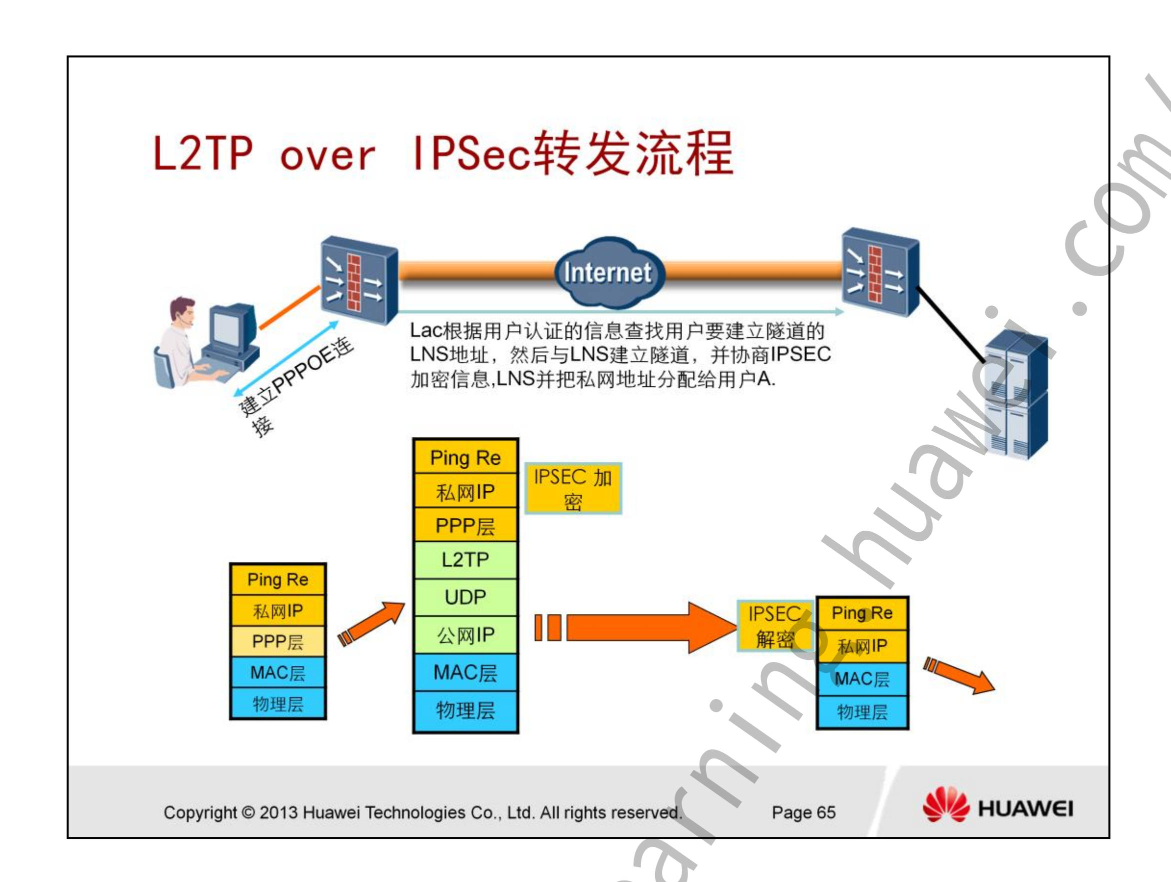



- 先做L2TP封装，再用IPSec加密；
- 只能使用IPSEC进行加密，认证和加密没有直接的关系。



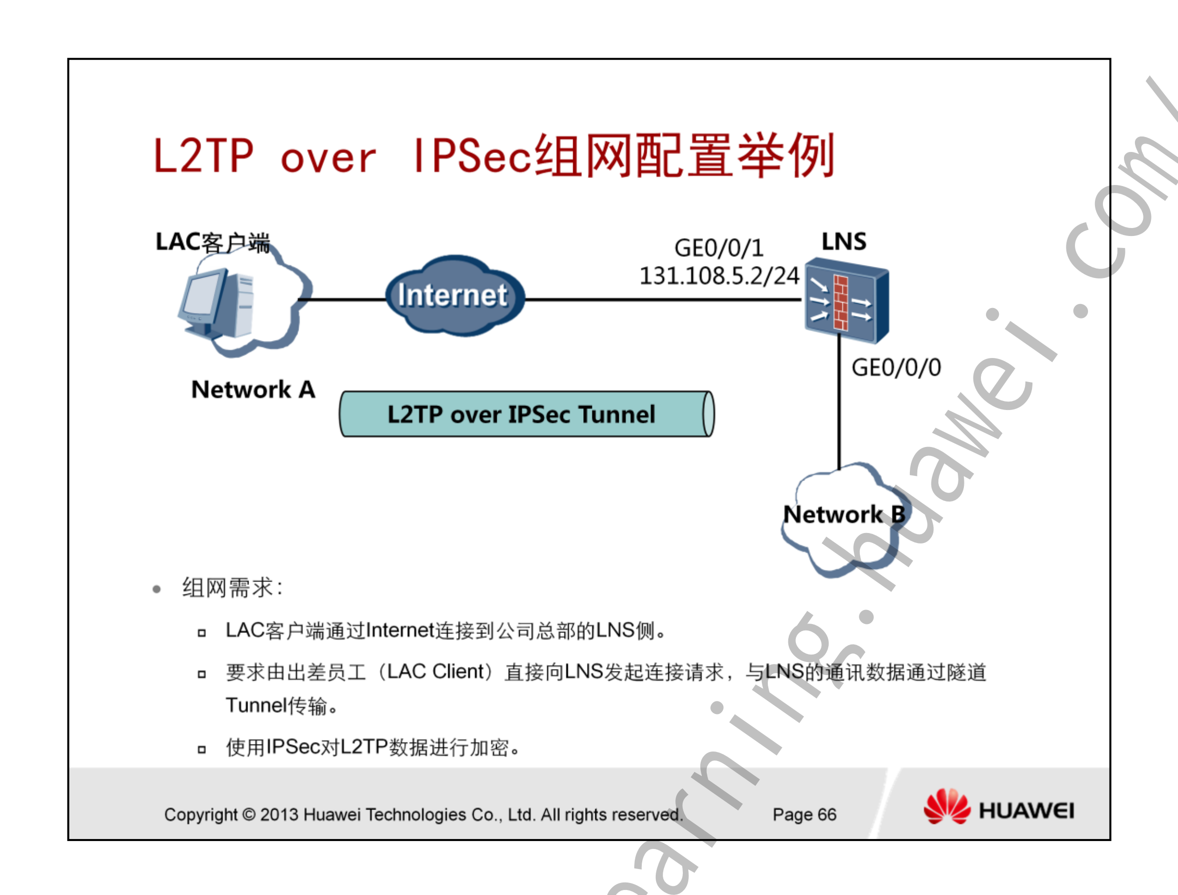




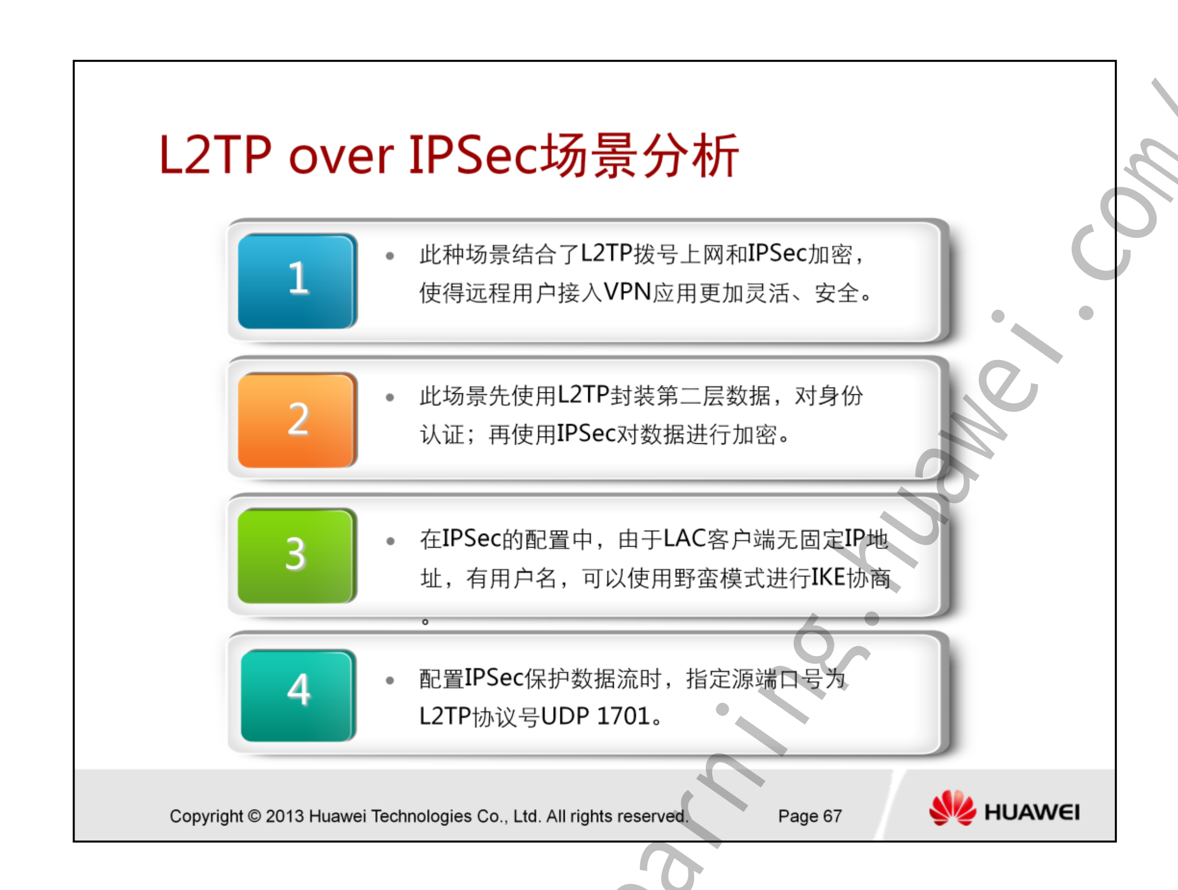



L2TP over IPSec VPN建立过程：

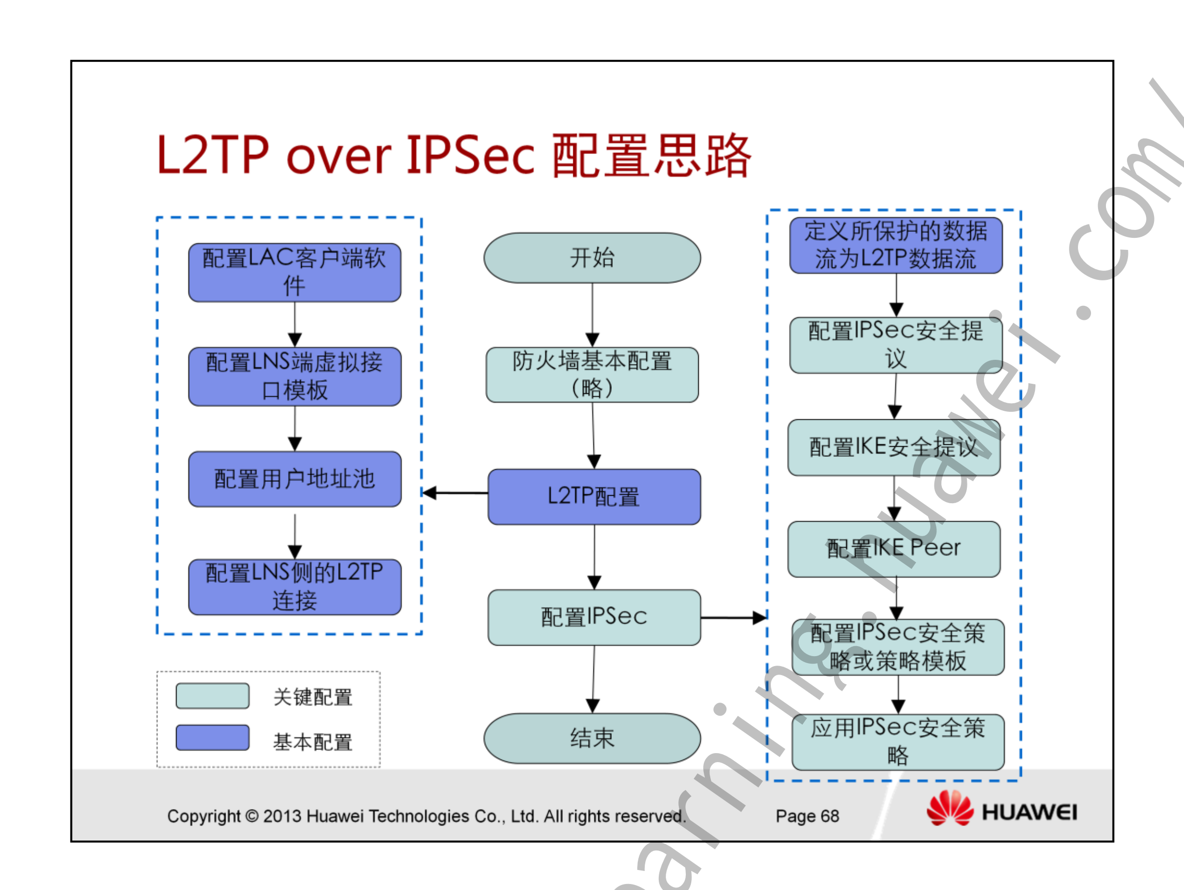
- 客户端拨号触发L2TP流量；
- L2TP流量触发IPSec VPN建立；
- L2TP流量被IPSec VPN封装并在公网上传输，并完成L2TP VPN协商与认证；
- L2TP over IPSec VPN建立完成，所有数据正常传输。




统的L2TP由于自身协议特点，存在安全隐患。配置L2TP over IPSec，即先用L2TP封装报文后再进行IPSec封装，可利用IPSec弥补L2TP的安全方面的不足，同时又利用L2TP弥补IPSec在用户认证、授权等方面的不足。




在IPSec配置中，除了可以采用野蛮模式进行IKE协商，同样可以配置IPSec 策略模板解决对端IP地址不固定的问题。




防火墙基础配置包括隧道两端网关的接口基本配置、安全域间包过滤配置和路由配置。

## L2TP over IPSec VPN关键配置

- 配置LNS侧的IPSec特性。 IKE协商模式为野蛮模式，并且设置remote-id为对端用户名client1。

  [LNS] **ike peer peer1**

  [LNS-ike-peer-peer1] **exchange-mode aggressive**

  [LNS-ike-peer-peer1] **local-id-type fqdn**

  [LNS-ike-peer-peer1] **ike-proposal 1**

  [LNS-ike-peer-peer1] **pre-shared-key abcde**

  [LNS-ike-peer-peer1] **remote-id client1**

- 定义IPSec保护数据流:

  [LNS] **acl number 3001**

  [LNS-acl-adv-3001] **rule permit udp source-port eq 1701**







Local-id-type命令用来配置IKE对等体的ID类型。可选择的参数有dn（表示ID类型为区别名的形式）、IP（表示ID类型为IP地址形式）、fqdn（表示ID类型为正式域名形式）、user-fqdn（表示ID类型为用户域名的形式）。

定义IPSec所保护数据流的ACL中，源端口号为L2TP的协议号。1701端口为LNS作为隧道响应端处理L2TP报文的端口。

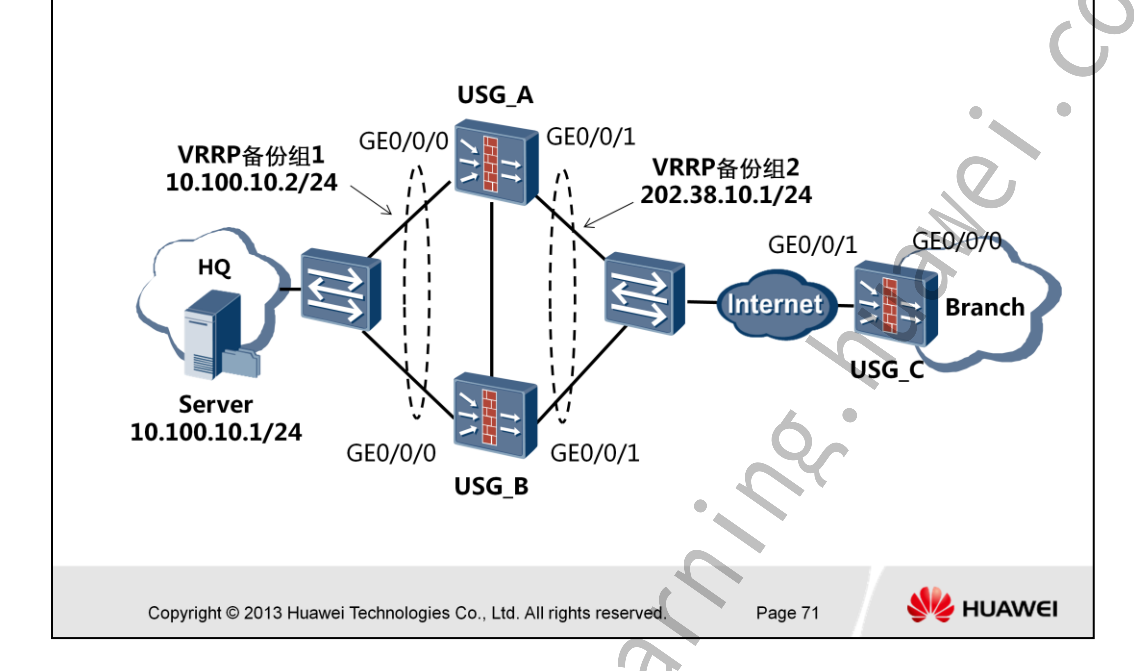


# 目录

1. VPN基础知识回顾
2. IPSec VPN典型应用介绍
3. L2TP Over IPSec应用分析
4. **SSL 应用分析**

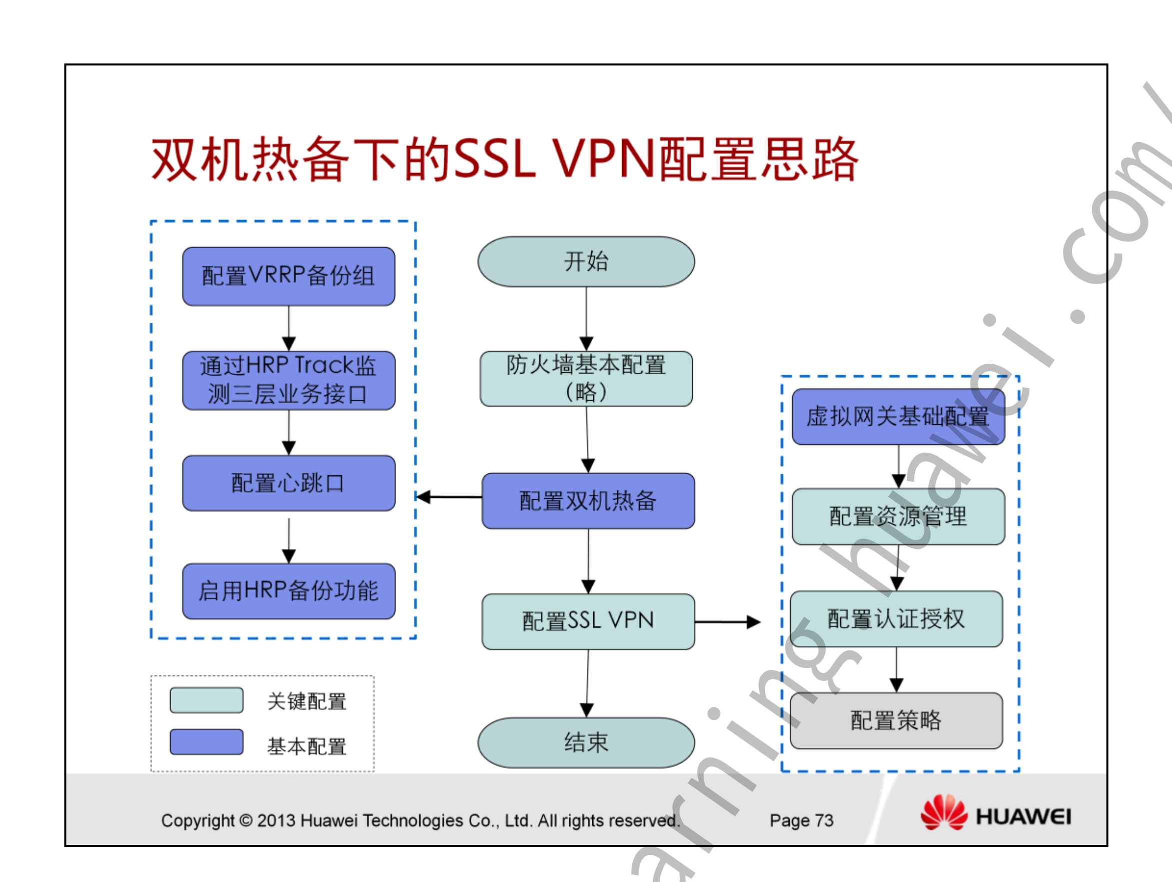






双机热备下的SSL VPN场景
USG_A
GE0/0/0
GE0/0/1
VRRP备份组1
10.100.10.2/24
VRRP备份组2
202.38.10.1/24
HQ
GE0/0/1
GE0/0/0
Internet
Branch
USG_C
Server
10.100.10.1/24
GE0/0/0
GE0/0/1
USG_B
HUAWEI




由于设备使用自身的MAC地址来进行通信，在采用主备方式的双机热备组网中，如果没有将网络扩展地址池与VRRP组号绑定，当主备切换时，内网服务器仍将报文发送至当前的备设备（即切换前的主设备），导致业务中断。直到内网服务器的ARP表刷新后，报文才会发送到当前主设备，网络再次连通，此时网络扩展业务才能被访问。将网络扩展地址池与VRRP组号绑定后，设备会使用VRRP的虚MAC地址来进行通信，避免了上述问题。


双机热备下的SSL VPN配置思路
配置VRRP备份组
通过HRP Track监测三层业务接口
配置心跳口
启用HRP备份功能
开始
防火墙基本配置（略）
配置双机热备
配置SSL VPN
结束
虚拟网关基础配置
配置资源管理
配置认证授权
配置策略
关键配置
基本配置
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 73
HUAWEI

# 关键配置（1）

虚拟网关的IP地址应为VRRP2的IP地址

VPN > SSL VPN > 虚拟网关管理

| | | |
|---|---|---|
| 虚拟网关名 | SSLVPN * | 字母、数字或下划线，1~15个字符 |
| 虚拟网关类型 | 独占 | |
| IP地址 | 202 . 38 . 10 . 1 * | 添加IP地址 |
| 虚拟网关域名 | | 示例: www.company.com(独占型)，vt1.company.com(共享型)，www.company.com/aa(共享型) |
| HTTP重定向 | 启用HTTP重定向服务 | |
| 最大并发用户数 | | 1~100，默认为系统限额（系统限额：100，当前剩余可用并发用户数：100） |
| 最大用户数 | 1 * | 1~1000，默认为1（系统限额：1000， 当前剩余可用用户数：1000） |
| 最大资源数 | 1 * | 1~1024，默认为1（系统限额：1024， 当前剩余可用资源数：1024） |

应用 返回



HUAWEI

在Web配置界面中，选择“VPN > SSL VPN > 虚拟网关管理”，单击“新建”。在IP地址一栏中，应该配置VRRP备份组公网接口的IP地址。

# 关键配置（2）




在主备方式的双机热备组网中，需在主备设备上分别配置“VRRP VRID”，将网络扩展地址池与VRRP组号绑定。



# 总结

- IPSec VPN高级特性及配置
- L2TP over IPSEC VPN高级特性及配置
- SSL VPN双机热备应用场景








# 思考题

1. 哪些安全协议可以支持NAT应用场景?
2. AH安全协议为何不支持NAT应用场景?
3. IPSec策略模板的主要应用于什么场景?
4. L2TP over IPSec中L2TP与IPSec之间是什么关系?








1. 哪些安全协议可以支持NAT应用场景?

   答题要点：ESP

2. AH安全协议为何不支持NAT应用场景?

   答题要点：AH协议对IP包头进行验证，由于NAT将IP头部信息转换，将会导致验证失败。

3. IPSec策略模板的主要应用于什么场景?

   答题要点：点到多点IPSec VPN

4. L2TP over IPSec中L2TP与IPSec之间是什么关系?

   答题要点：数据包进行封装时，首先封装L2TP，然后封装IPSec。



# 练习题

- 判断题

  1.L2TP over IPSec是指IPSec VPN通过ACL包含的感兴趣流触发L2TP VPN的建立。

- 单选题

  1.以下哪个安全协议可支持在NAT应用场景?

  A. ESP　　B. AH　　C. AH+ESP　　D. 其它都支持







习题与答案:

1. L2TP over IPSec是指IPSec VPN通过ACL包含的感兴趣流触发L2TP VPN的建立。

答案：错误

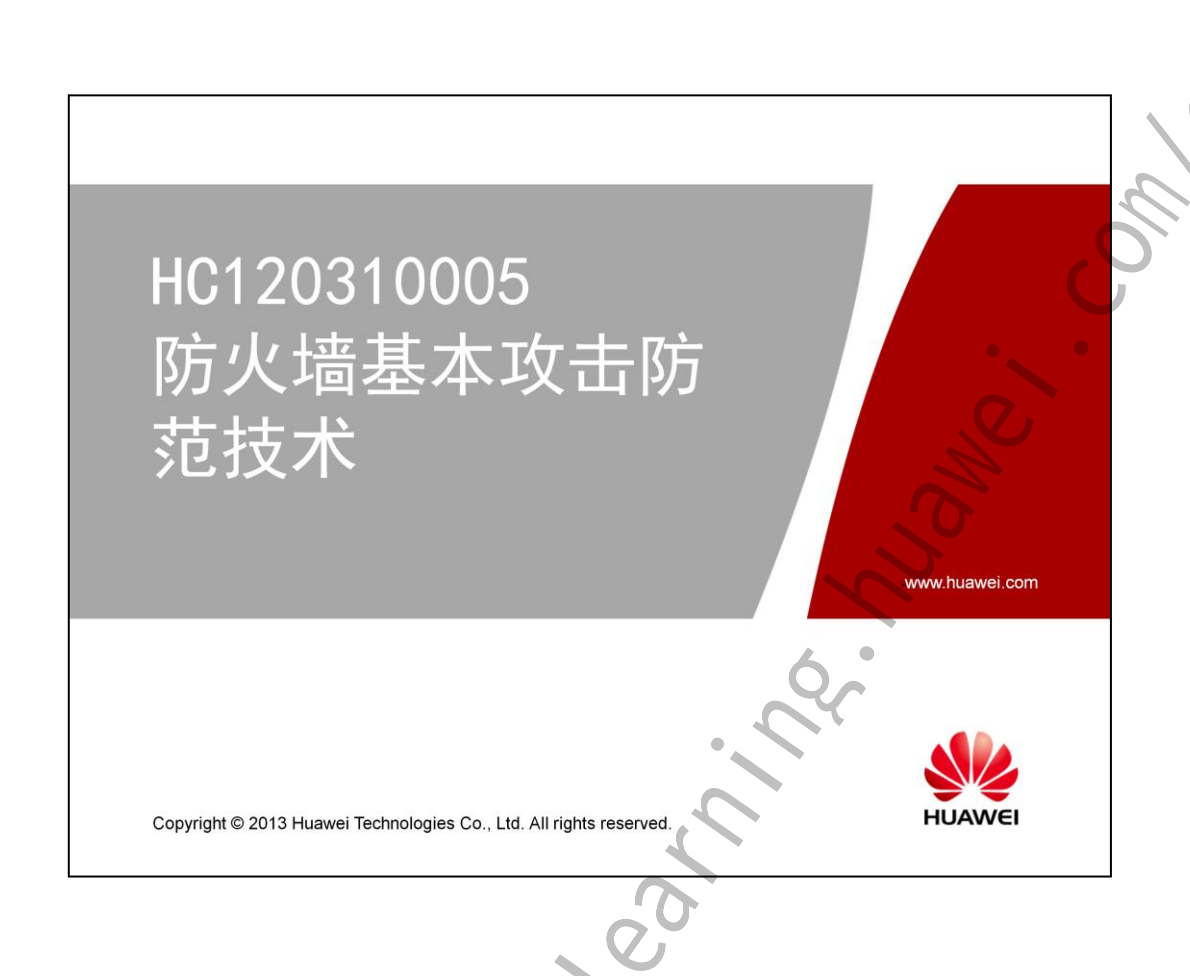
2. 以下哪个安全协议可支持在NAT应用场景?

A. ESP　　B. AH　　C. AH+ESP　　D. 其它都支持

答案：A

Thank You

www.huawei.com


HC120310005
防火墙基本攻击防范技术
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



# 目标

- 学完本课程后，您将能够:
  - 了解基本的网络攻击
  - 掌握防火墙基本攻击防范技术
  - 熟悉防火墙基本攻击防范应用与配置







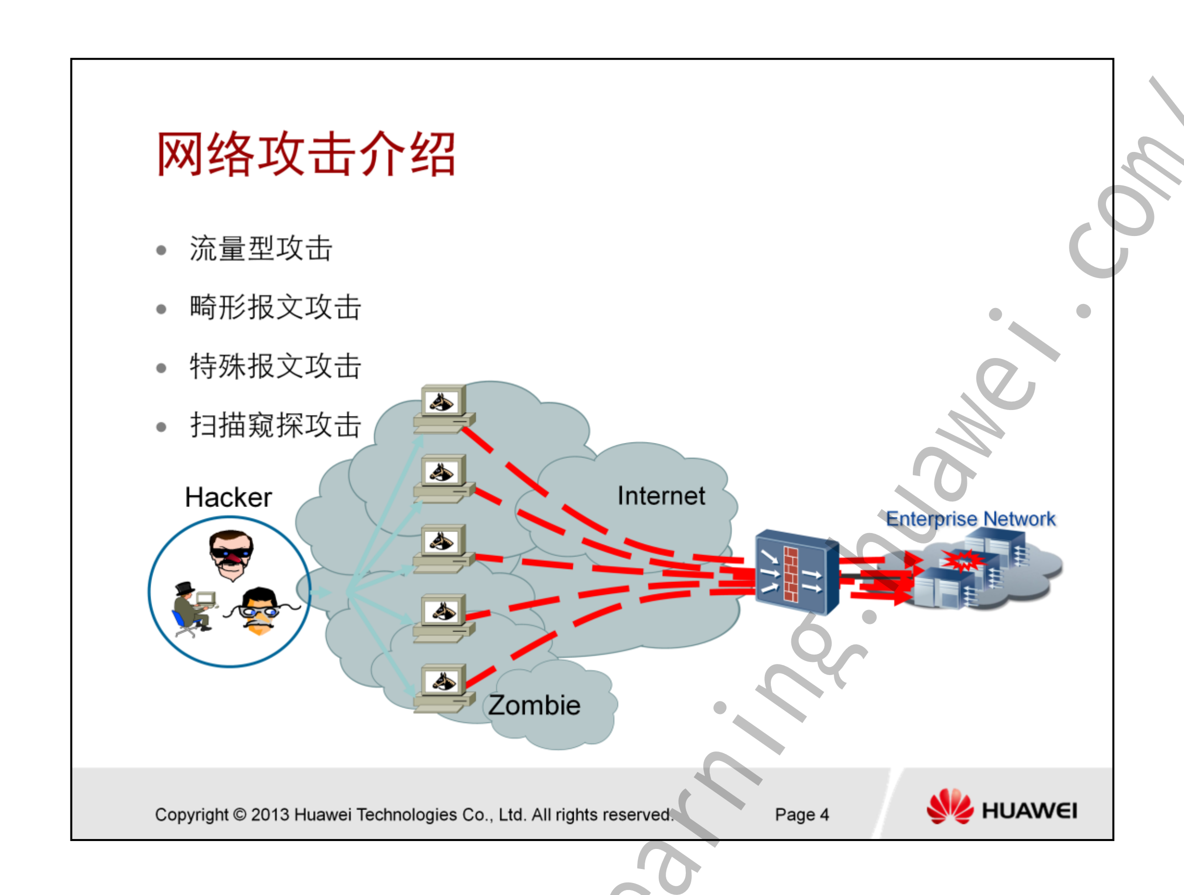
# 目录

1. **网络攻击介绍**
2. 防火墙攻击防范通用技术
3. 防火墙攻击防范应用



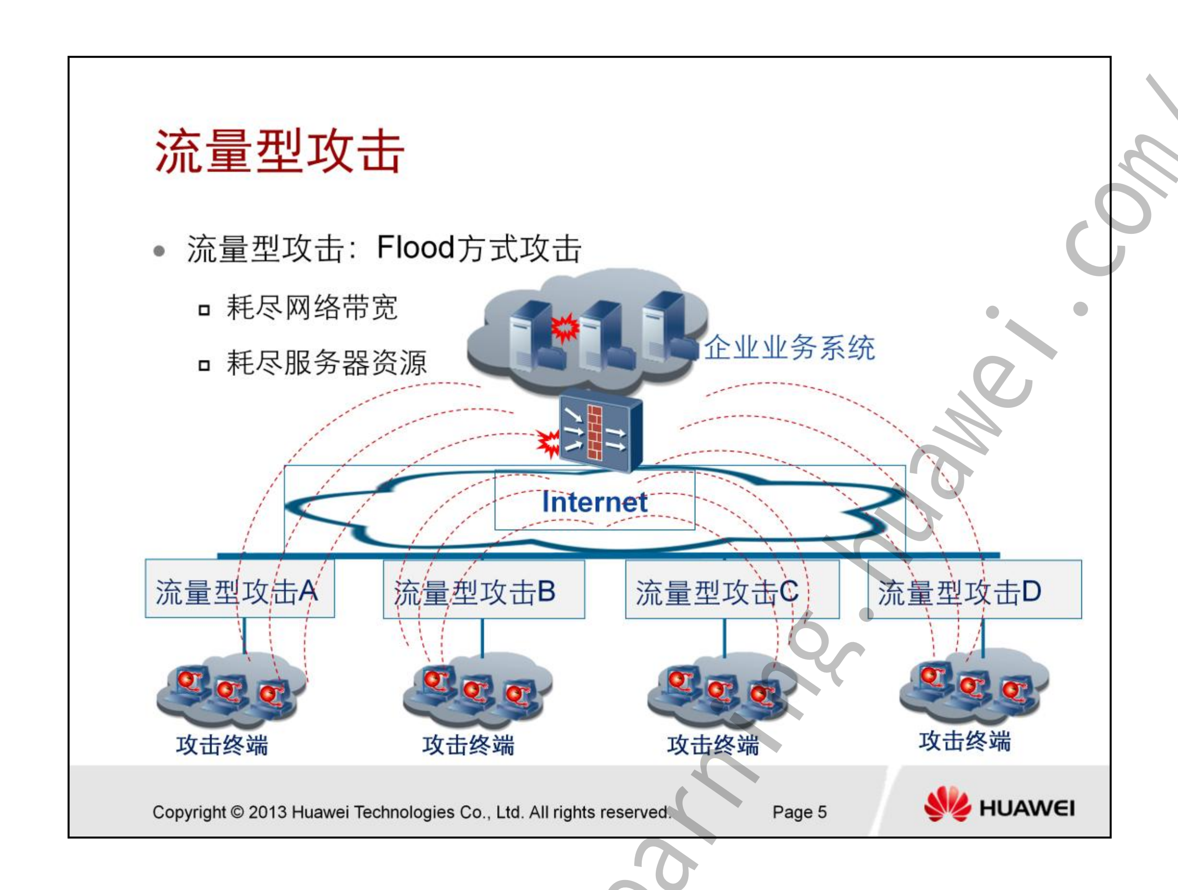






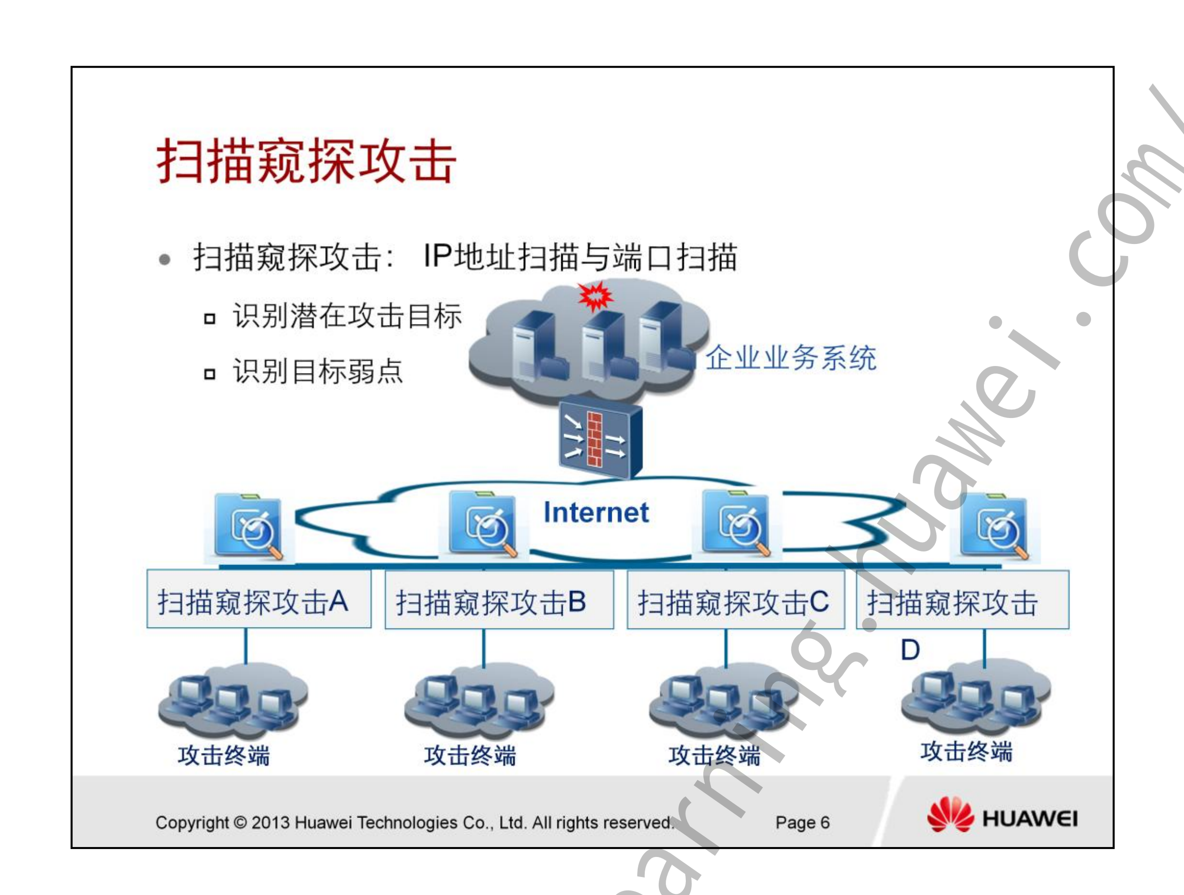

通常的网络攻击，一般是侵入或破坏网上的服务器（主机），盗取服务器的敏感数据或占用网络带宽，干扰破坏服务器对外提供的服务。也有直接破坏网络设备的网络攻击，这种破坏影响较大，会导致网络服务异常，甚至中断。

网络攻击主要分为流量型攻击，扫描窥探攻击，畸形报文攻击和特殊报文攻击。

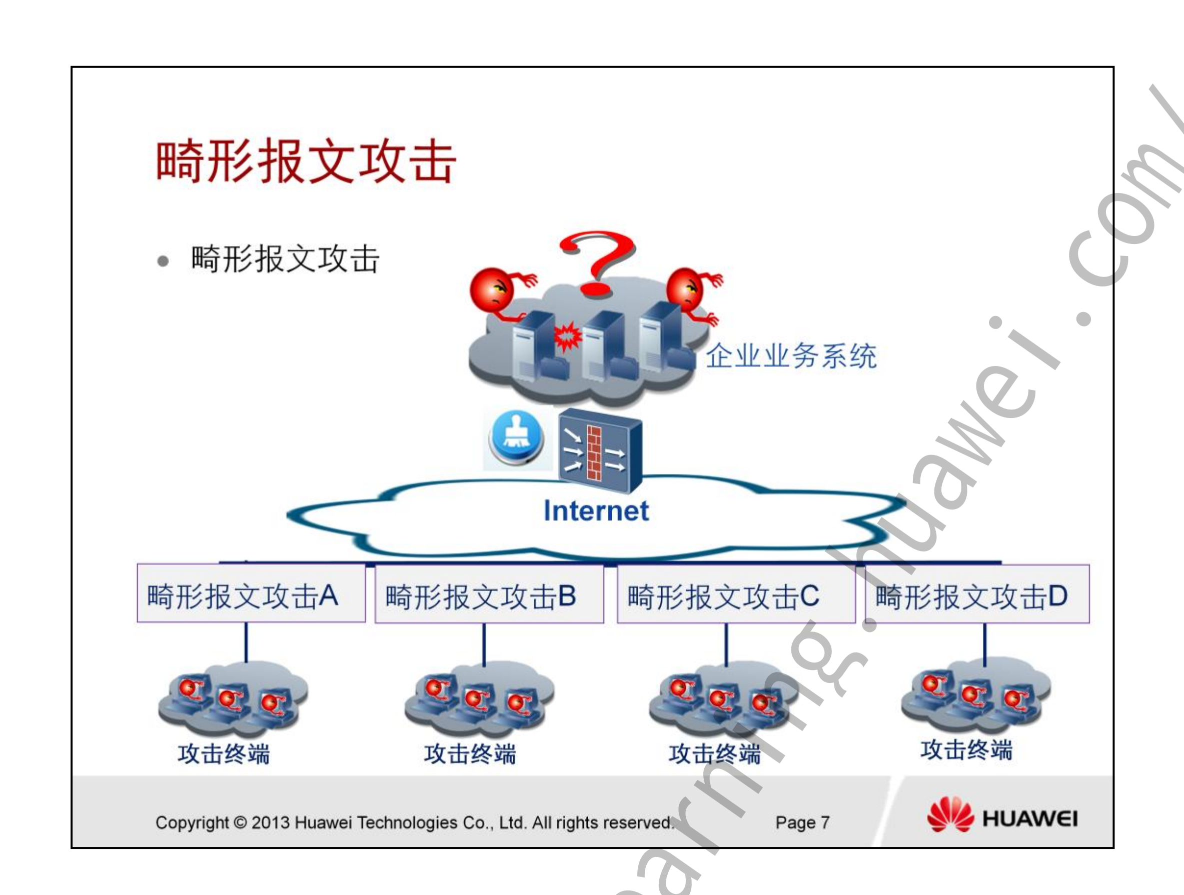



流量型攻击是指攻击者通过大量的无用数据占用过多的资源以达到服务器拒绝服务的目的。

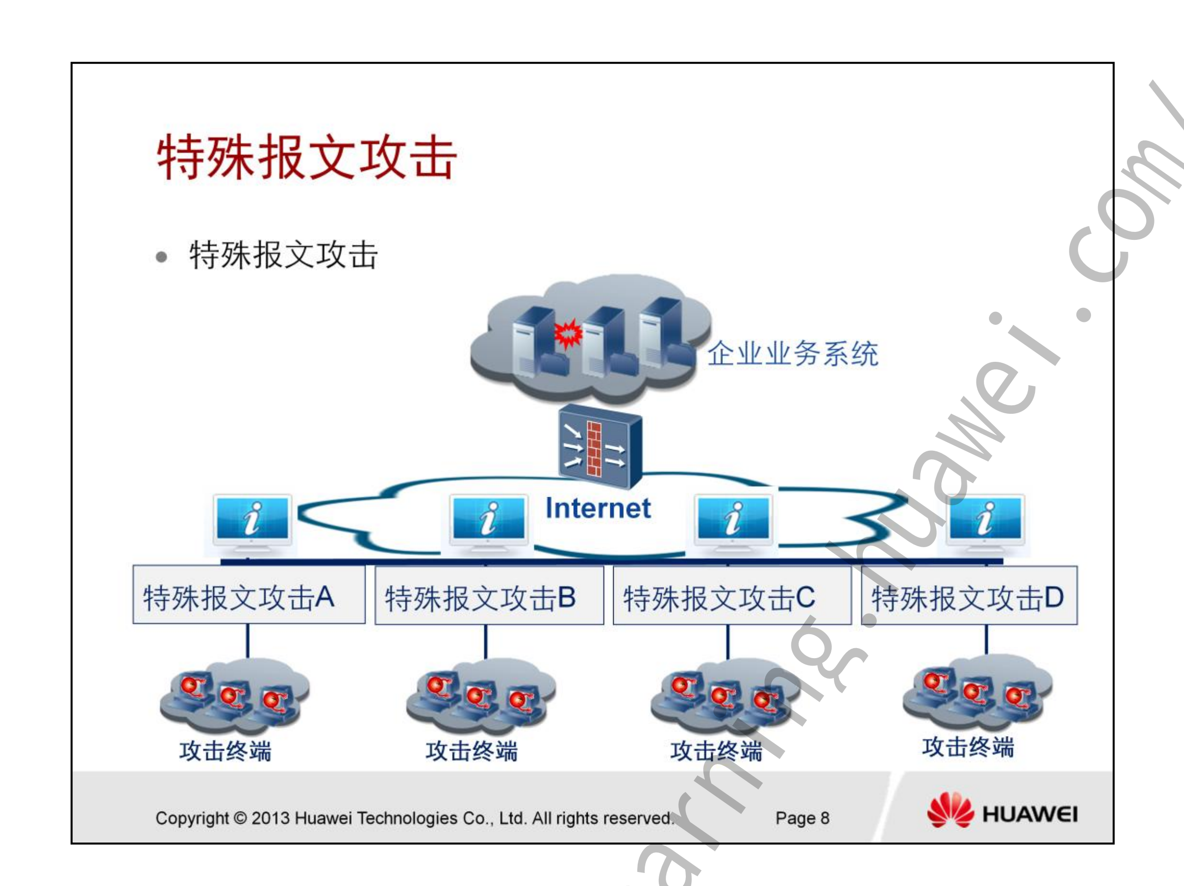
这类攻击典型特征是通过发出海量数据包，造成设备负载过高，最终导致网络带宽或是设备资源耗尽。通常，被攻击的路由器、服务器和防火墙的处理资源都是有限的，攻击负载之下它们就无法处理正常的合法访问，导致正常服务被拒绝。流量型攻击最通常的形式是Flood方式，这种攻击把大量看似合法的TCP、UDP、ICMP包发送至目标主机，甚至，有些攻击者还利用源地址伪造技术来绕过检测系统的监控，以达到攻击的目的。




扫描窥探攻击是利用ping扫射（包括ICMP和TCP）来标识网络上存活着的系统，从而准确清楚潜在的目标；利用TCP和UDP端口扫描，就能检测出操作系统和监听着的潜在服务。攻击者通过扫描窥探就能大致了解目标系统提供的服务种类和潜在的安全漏洞，为进一步侵入系统做好准备。




畸形报文攻击是指通过向目标系统发送有缺陷的IP报文，使得目标系统在处理这样的IP报文时发生错误，或者造成系统崩溃，影响目标系统的正常运行。主要的畸形报文攻击有Ping of Death、Teardrop等。




特殊报文攻击是指攻击者利用一些合法的报文对网络进行侦察或者数据检测，这些报文都是合法的应用类型，只是正常网络很少用到。



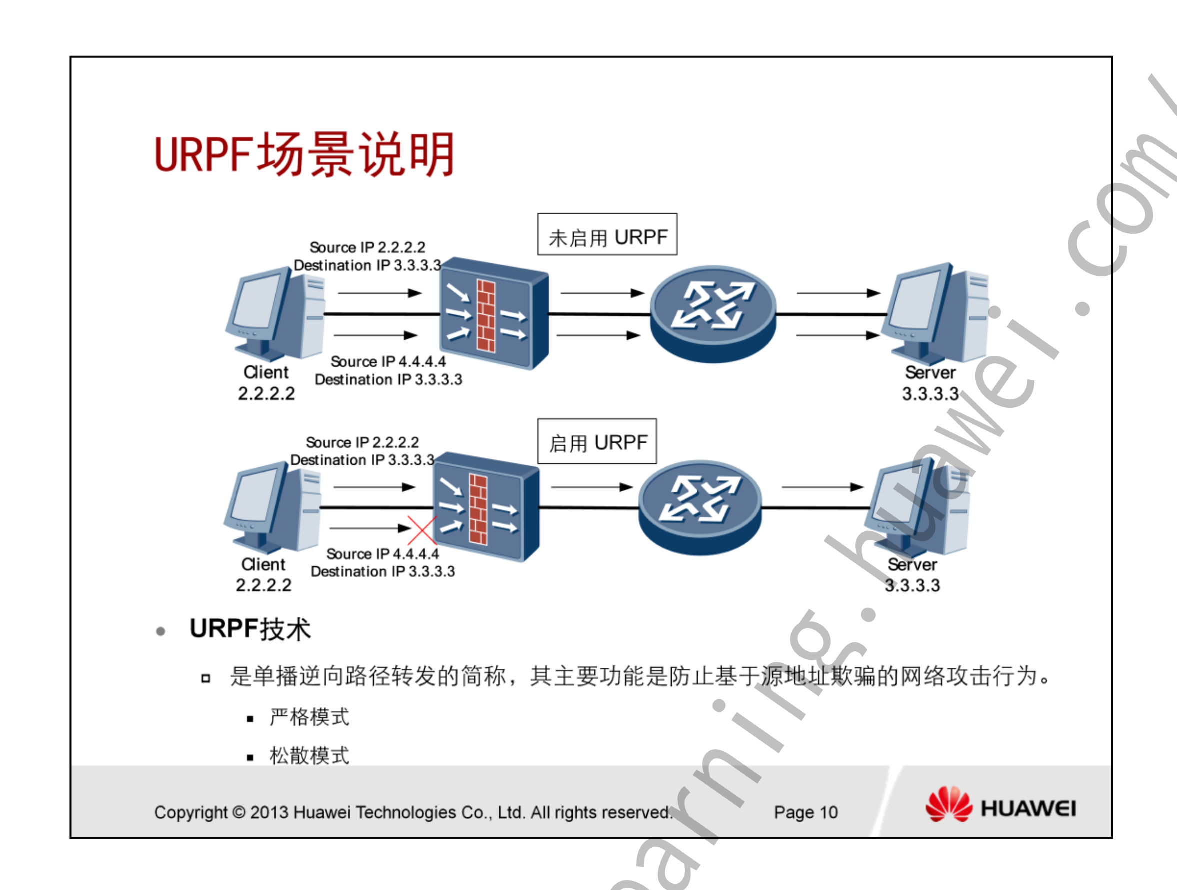
# 目录












- 严格模式

建议在路由对称的环境下使用URPF严格模式，即：不仅要求在转发表中存在相应表项，还要求接口一定匹配才能通过URPF检查。

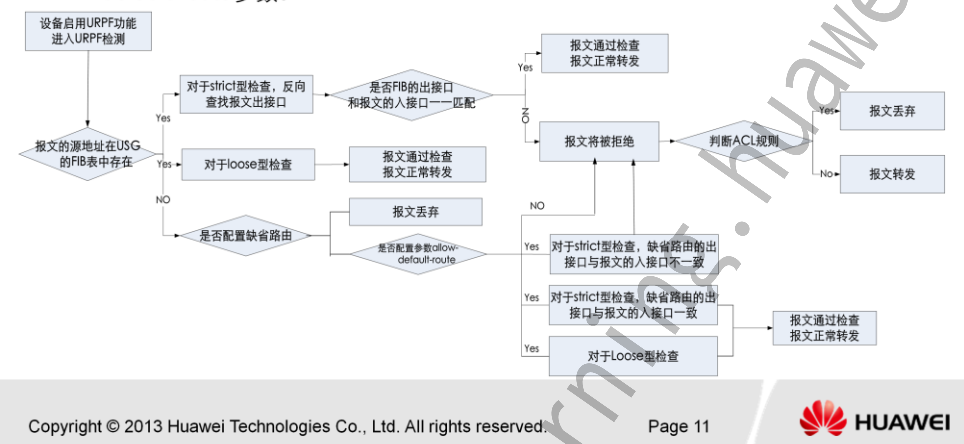
如果两个网络边界路由器（此处为USG）之间只有一条路径的话，这时，路由能够保证是对称的，使用严格模式能够最大限度的保证网络的安全性。

- 松散模式

在不能保证路由对称的环境下使用URPF的松散模式，即：不检查接口是否匹配，只要存在针对源地址的路由，报文就可以通过。

## URPF处理流程

- URPF的处理流程如下：
  - 如果报文的源地址在USG的FIB表中存在。
  - 如果报文的源地址在USG的FIB表中不存在，则检查缺省路由及URPF的allow-default-route参数。




URPF的处理流程:

- 如果报文的源地址在USG的FIB表中存在。
  - strict型检查，反向查找报文出接口，若只有一个出接口和报文的入接口一一对于匹配，则报文通过检查；否则报文将被拒绝。当有多个出接口和报文的入接口相匹配时，必须使用loose型检查。
  - 对于loose型检查，当报文的源地址在USG的FIB表中存在（不管反向查找的出接口和报文的入接口是否一致），报文就通过检查；否则报文将被拒绝。
- 如果报文的源地址在USG的FIB表中不存在，则检查缺省路由及URPF的allow-default-route参数。
  - 对于配置了缺省路由，但没有配置参数allow-default-route的情况。只要报文的源地址在USG的FIB表中不存在，该报文都将被拒绝。
  - 对于配置了缺省路由，同时又配置了参数allow-default-route的情况。
    - 如果是strict检查，只要缺省路由的出接口与报文的入接口一致，则报文将通过URPF的检查，进行正常的转发。如果缺省路由的出接口和报文的入接口不一致，则报文将拒绝。
    - 如果是loose型检查，报文都将通过URPF的检查，进行正常的转发。

## URPF处理流程

- 当且仅当报文被拒绝后，才去匹配ACL列表。如果被ACL允许通过，则报文继续进行正常的转发；如果被ACL拒绝，则报文被丢弃。
- URPF配置：
  - 进入接口视图

```
[USG] interface interface-type interface-number
```

  - 启用接口URPF功能

```
ip urpf { loose | strict } [ allow-default-route ] [ acl acl-number ] （IPv4）
ipv6 urpf { loose | strict } [ allow-default-route ] [ acl6 acl-number ] （IPv6）
```






- 操作步骤

执行命令system-view，进入系统视图。

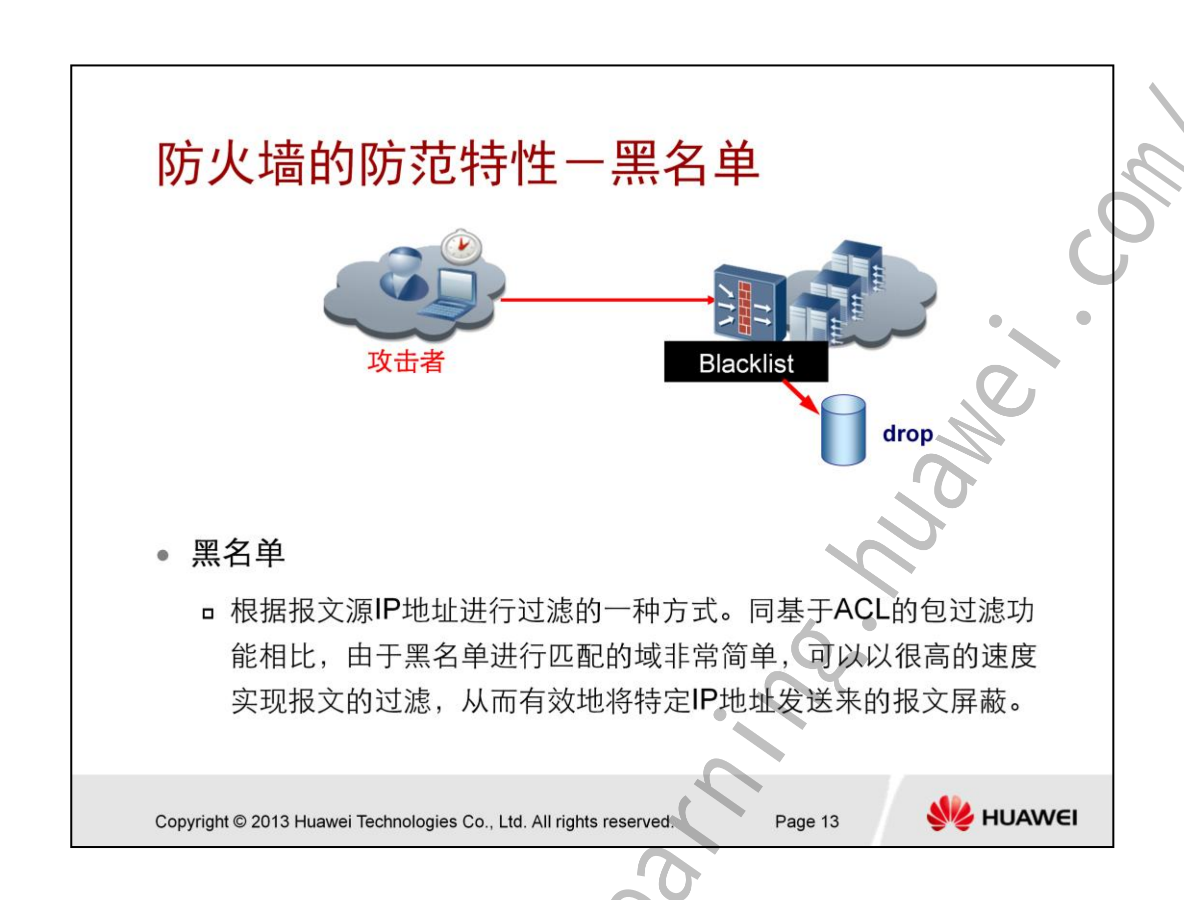
执行命令interface interface-type interface-number，进入接口视图。

可以使能URPF功能的接口包括GE接口、VLAN IF接口、Eth-Trunk接口、Tunnel接口和子接口。

使能接口URPF功能。

IPv4网络中执行命令ip urpf { loose | strict } [ allow-default-route ] [ acl acl-number ]

IPv6网络中执行命令ipv6 urpf { loose | strict } [ allow-default-route ] [ acl6 acl-number ]




黑名单最主要的一个特色是可以由USG防火墙动态地进行添加或删除，当防火墙中根据报文的行为特征察觉到特定IP地址的攻击企图之后，通过主动修改黑名单列表从而将该IP地址发送的报文过滤掉。因此，黑名单是防火墙一个重要的安全特性。

## 防火墙的防范特性—黑名单

- 黑名单功能一般和IP扫描，port扫描，ACL等攻防命令配置使用，动态的添加删除黑名单内容，也可以静态手工添加黑名单内容
- 黑名单配置：
  - 配置黑名单功能

```
[USG]firewall blacklist enable
```

  - 静态手工添加黑名单

```
[USG] firewall blacklist item 202.169.168.1 timeout 100
```







- 命令

**firewall blacklist** { **enable** [ **acl-number** *acl-number* ] | **item** *source-address* [ [ **timeout***interval* ] **vpn-instance** *vpn-instance-name* ] |

**filter-type { icmp | tcp | udp | others } }**

**undo firewall blacklist { enable | item [ [ source-address ] [ vpn-instance vpn-instancename] | filter-type [ icmp | tcp | udp | others ] }**

- 参数

**enable**：使能黑名单功能 **acl-number** *acl-number* **item** *source-address*：指定添加到黑名单的IP 地址。

**filter-type**：黑名单过滤类型，包括四个参数**icmp**、**tcp**、**udp** 和**other**，分别表示过滤ICMP 报文、TCP 报文、UDP 报文和其他报文四种类型。

# 防火墙的防范特性—黑名单








HUAWEI

1. 选择“防火墙 > 安全防护 > 黑名单”。
2. 在“配置黑名单”界面，选中“黑名单功能”对应的“启用”复选框。
3. 配置黑名单绑定ACL号，参数说明请参见表1。
4. 单击“应用”。
5. 在“黑名单列表”界面中，查看黑名单表项信息。

# IP—MAC地址绑定

- **IP – MAC地址绑定**
  - 只有完全匹配IP和MAC的报文才能进入防火墙的下一个处理流程，不匹配的报文将被丢弃。
- **IP – MAC地址绑定配置**

  \# 配置客户机IP地址和MAC地址到地址绑定关系中。

  ```
  [USG] firewall mac-binding 202.169.168.1 00e0-fc00-0100
  ```

  \# 使能地址绑定功能。

  ```
  [USG] firewall mac-binding enable
  ```

报文即不匹配IP，也不匹配MAC，能否通过防火墙?








- 【参数】

  enable：使能地址绑定功能。source-address：指定地址绑定对的IP 地址。mac-address：指定地址绑定对的MAC 地址。vpn-instance vpn-instance- name：配置指定VPN 实例的地址绑定信息。

  all：全部地址绑定对。

- 【举例】

  # 在地址绑定表项中插入一条IP 地址为192.168.10.10，MAC 地址为00e0-0000-0001的地址绑定表项。

  [USG] firewall mac-binding 192.168.10.10 00e0-0000-0001

  # 在地址表项中为VPN 实例v1 插入一条IP 地址为192.168.2.2，MAC 地址为1234-5678-9012 的地址绑定表项。

  [USG] firewall mac-binding 192.168.2.2 1234-5678-9012 vpn-instance v1

  # 使能地址绑定功能。

  [USG] firewall mac-binding enable

## IP—MAC地址绑定

防火墙 > 安全防护 > IP-MAC绑定

配置IP-MAC地址绑定

IP-MAC地址绑定功能 ☐ 启用 应用

①启用IP-Mac绑定功能

IP-MAC地址绑定列表

新建 删除 刷新 查询

IP地址 MAC地址

②新建IP-Mac绑定列表

第 1 页共 1 页

防火墙 > 安全防护 > IP-MAC绑定

新建IP-MAC地址绑定

IP地址 *

MAC地址 *

VLAN ID <1-4094>

应用 返回

③设置IP和Mac地址





HUAWEI

- IP-MAC绑定

  通过配置MAC和IP地址绑定，可以防止IP仿冒。

  IP-MAC绑定是指MAC（Media Access Control）和IP地址绑定，设备根据用户的配置，在IP地址和MAC地址之间形成关联关系。对于声称源地址为这个IP地址的报文，如果其MAC地址不是指定关系对中的MAC地址，设备将予以丢弃。目的地址为这个IP地址的报文，在通过设备时将被强制发送到MAC-IP地址关联关系中，该IP地址对应的MAC地址，从而对用户形成有效的保护。

- 操作步骤

  选择“防火墙 > 安全防护 > IP-MAC绑定”。

  在“配置IP-MAC地址绑定”界面中，开启地址绑定功能。

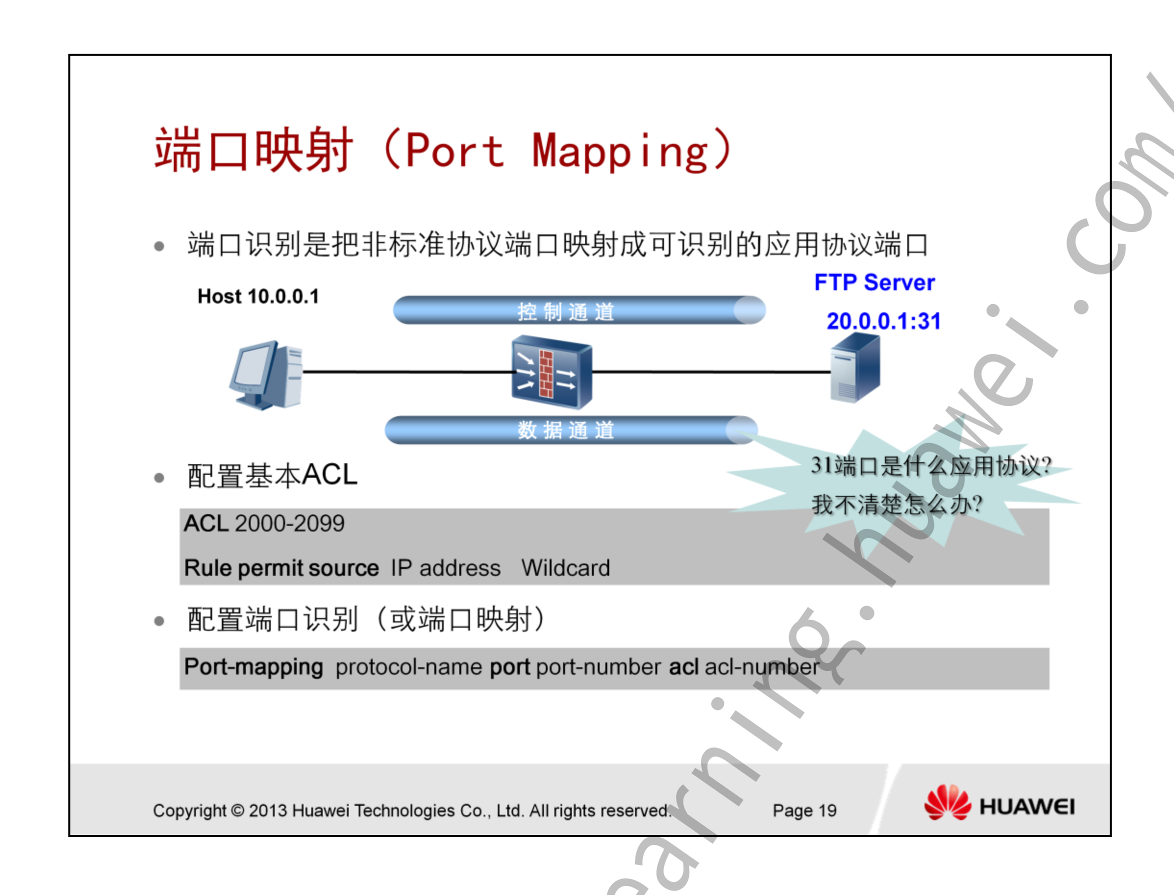
  选中“启用”对应的复选框。

  单击“应用”。

  在“IP-MAC地址绑定列表”界面中，配置MAC和IP地址绑定。

  单击“新建”，配置IP-MAC地址绑定的各参数，参数说明请参见表1。

  单击“应用”。




端口识别，也称端口映射，是防火墙用来识别使用非标准端口的应用层协议报文。端口映射支持的应用层协议包括FTP、HTTP、RTSP、PPTP、MGCP、MMS、SMTP、H323、SIP、SQLNET。

端口识别基于ACL进行，只有匹配某条ACL的报文，才会实施端口映射。端口映射使用基本ACL（编号2000～2999）。端口映射在使用ACL过滤报文时，使用报文的目的IP地址去匹配基本ACL中配置的源IP地址。

ACL(Access Control List),访问控制列表是一系列有顺序的规则组的集合，这些规则根据数据包的源地址、目的地址、端口号等来描述。ACL通过规则对数据包进行分类，这些规则应用到路由设备上，路由设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

ACL分为以下四类：

- 基本ACL（2000～2999）：只能通过源IP地址和时间段来进行流量匹配，在一些只需要进行简单匹配的功能可以使用。
- 高级ACL（3000～3999）：通过源IP地址、目的IP地址、ToS、时间段、协议类型、优先级、ICMP报文类型和ICMP报文码等多个维度来对进行流量匹配，在大部分功能中都可使用高级ACL来进行精确流量匹配。
- 基于MAC地址的ACL（4000～4999）：可以通过源MAC地址、目的MAC地址、CoS、协议码等维度来进行流量匹配。

# 端口映射（Port Mapping）

服务映射列表：防火墙 > 服务 > 服务映射

| 端口 | 目的地址 |
| --- | --- |

①新建服务映射列表

新建服务映射

| 参数 | 值 |
| --- | --- |
| 协议 | FTP * |
| 自定义端口号 | * <0-65535> |
| 目的地址 | any |
| 时间段 | all |
| 动作 | permit |

应用　返回

②设置映射协议和自定义端口号

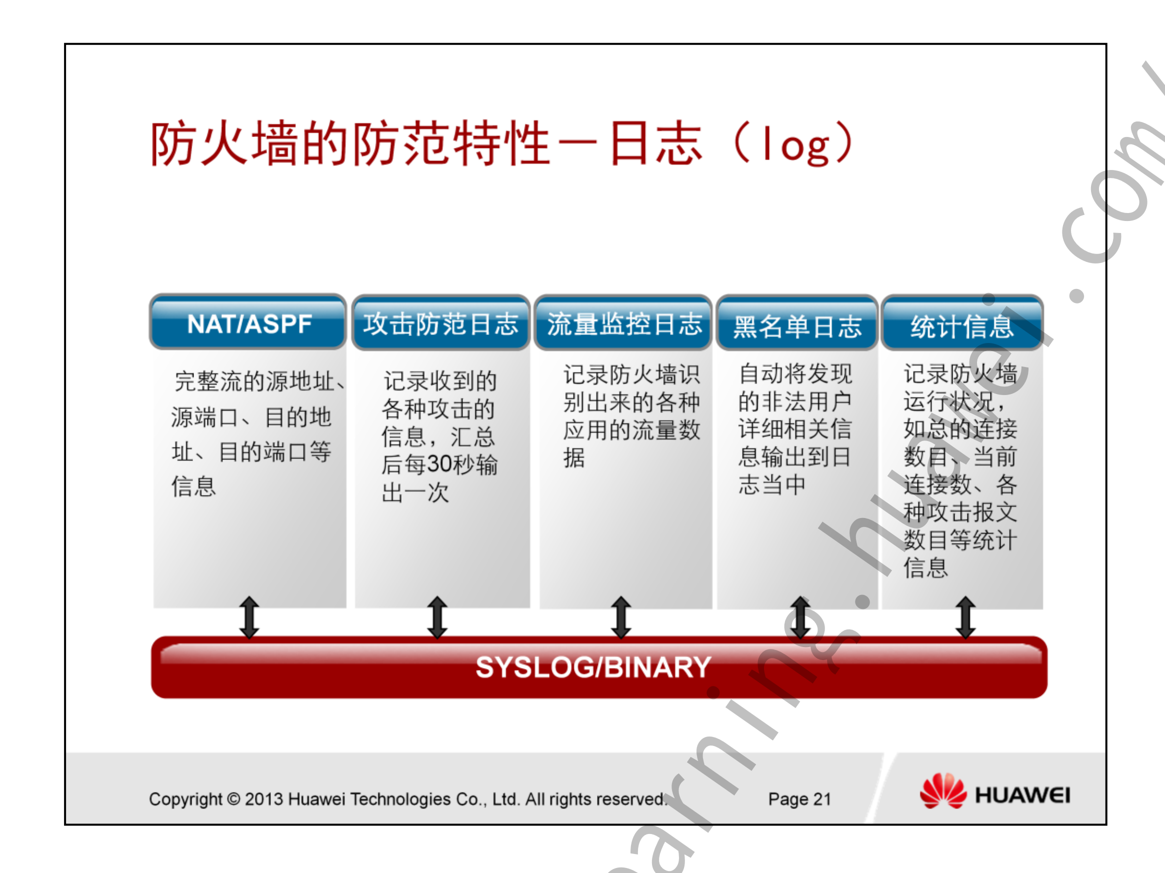


HUAWEI

服务映射

应用层协议一般使用知名端口号进行通信，例如FTP使用20和21端口，Web服务通常使用80端口。但是在某些情况下，内网服务器需要通过其他自定义端口对外提供知名服务时，可以通过服务映射功能来完成相应的转换。

1. 选择“防火墙 > 服务 > 服务映射”。
2. 在“服务映射列表”中，单击“新建”。
3. 依次输入或选择各项参数，如表1所示。
4. 单击“应用”。




USG防火墙提供完整、统一的日志信息描述，日志类型包括：

- **NAT日志和ASPF流日志**

日志内容中包含一个完整流的源地址、源端口、目的地址、目的端口等信息，及流的开始和结束时间、流的状态信息等。对于使用NAT功能的流还标识了地址转换之后的地址和端口信息。

- **攻击防范日志**

当发生大量攻击时，USG防火墙利用队列机制对防火墙支持的攻击防范特性提供日志告警信息，通过SYSLOG方式输出告警，告警信息包括攻击来源（源地址）和攻击种类等。

- **流量监控日志**

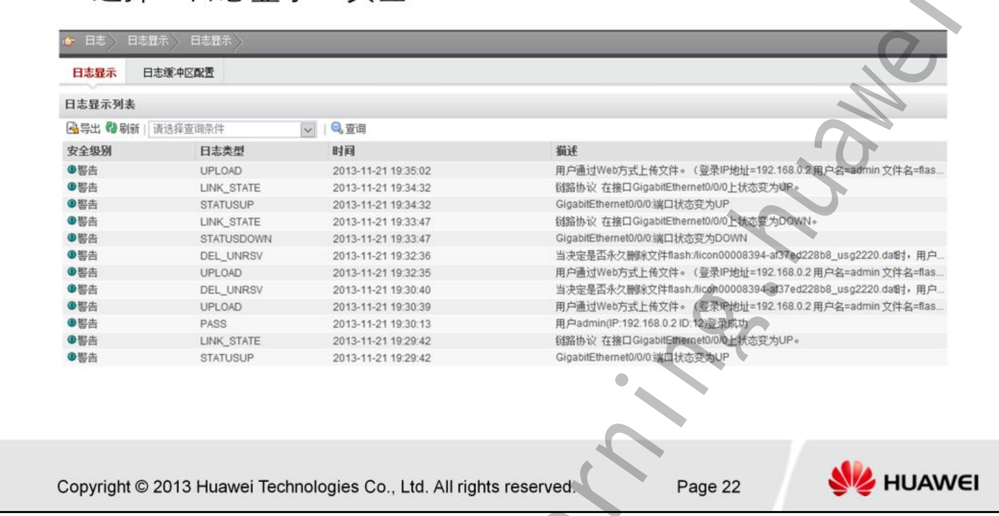
USG防火墙根据安全域、IP地址等参数进行流量监控，判断速率或连接数目是否达到上限或下限值，当达到上限时触发告警并记录日志，从而有效监控流量；当达到下限时，也触发告警，指示系统恢复正常。

- **黑名单日志**

USG防火墙对于在检测中发现的非法用户，自动将该用户的源IP地址加入到黑名单中，并产生一条黑名单日志，该日志记录主机地址、加入原因等信息。

- **多种统计信息**

记录流统计信息，了解防火墙运行状况。这些流统计信息包括：总的连接数目、当前连接及半连接数目、最高峰值及丢弃报文数目。记录各种攻击报文的数目。




| 安全级别 | 日志类型 | 时间 | 描述 |
|---|---|---|---|
| 警告 | UPLOAD | 2013-11-21 19:35:02 | 用户通过Web方式上传文件。（登录IP地址=192.168.0.2 用户名=admin 文件名=flas... |
| 警告 | LINK_STATE | 2013-11-21 19:34:32 | 链路协议 在接口GigabitEthernet0/0/0上状态变为UP。 |
| 警告 | STATUSUP | 2013-11-21 19:34:32 | GigabitEthernet0/0/0:端口状态变为UP |
| 警告 | LINK_STATE | 2013-11-21 19:33:47 | 链路协议 在接口GigabitEthernet0/0/0上状态变为DOWN。 |
| 警告 | STATUSDOWN | 2013-11-21 19:33:47 | GigabitEthernet0/0/0:端口状态变为DOWN |
| 警告 | DEL_UNRSV | 2013-11-21 19:32:36 | 当决定是否永久删除文件flash:/licon00008394-af37ed228b8_usg2220.dat时，用户... |
| 警告 | UPLOAD | 2013-11-21 19:32:35 | 用户通过Web方式上传文件。（登录IP地址=192.168.0.2 用户名=admin 文件名=flas... |
| 警告 | DEL_UNRSV | 2013-11-21 19:30:40 | 当决定是否永久删除文件flash:/licon00008394-af37ed228b8_usg2220.dat时，用户... |
| 警告 | UPLOAD | 2013-11-21 19:30:39 | 用户通过Web方式上传文件。（登录IP地址=192.168.0.2 用户名=admin 文件名=flas... |
| 警告 | PASS | 2013-11-21 19:30:13 | 用户admin(IP:192.168.0.2 ID:12)登录成功 |
| 警告 | LINK_STATE | 2013-11-21 19:29:42 | 链路协议 在接口GigabitEthernet0/0/0上状态变为UP。 |
| 警告 | STATUSUP | 2013-11-21 19:29:42 | GigabitEthernet0/0/0:端口状态变为UP |

- **日志种类划分**

普通系统日志

普通系统日志包括包过滤日志、HTTP访问日志、攻击防范日志、黑名单日志、地址绑定日志、入侵检测日志、防病毒日志、URL过滤日志等。

会话日志

会话日志主要是包括NAT/ASPF等的会话信息日志，支持Syslog和二进制两种输出方式。

流量监控日志

流量监控日志包括基础流量日志、应用流量日志、DPI流量监控日志和接口流量日志等。

- **日志输出原理**

根据日志输出方式的不同可以分为Syslog日志、二进制日志：

Syslog日志

像普通系统日志以及流量监控日志（除DPI流量监控日志外）采用Syslog方式以文本格式进行输出。这些日志信息必须通过信息中心模块进行日志管理和输出重定向，然后显示在终端屏幕上，或者发送给日志主机进行存储和分析。

二进制日志

像会话日志中NAT/ASPF产生的日志、DPI流量监控日志，对于这种类型的日志提供了一种“二进制”输出方式，直接输出到二进制日志主机以便对日志进行存储和分析，无需信息中心模块的参与。相比较而言，二进制日志的传输效率高于Syslog日志。

## 防火墙的防范特性—联动

- 攻击防范联动
  - 由于防火墙自身具有一定的局限性，如检查的颗粒度较粗，难以对众多的协议细节进行深入的分析与检查，并且防火墙具有防外不防内的特点，难以对内部用户的非法行为和已经渗透的攻击进行有效的检查和防范。因此，USG防火墙开放了相关接口，通过与其它安全软件进行联动，从而构建统一的安全网络。
- 目前支持联动的设备
  - 支持与SIG联动功能；
  - 支持与NIP联动功能；
  - 支持与TSM联动；
  - 支持其他厂商的IDS联动。

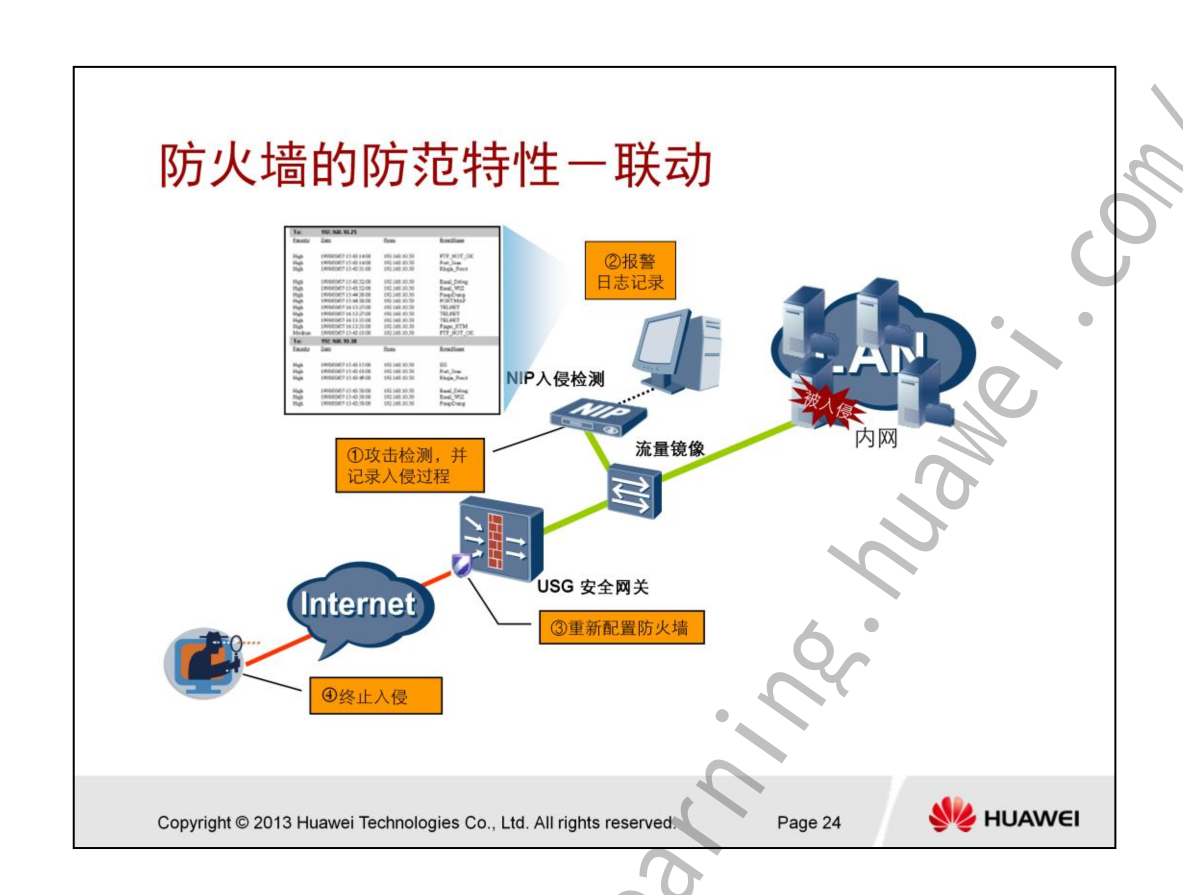





一般情况下，为了确保系统的通信性能不受安全设备的影响太大，IDS设备不能像防火墙一样置于网络入口处，只能置于旁路位置。而在实际使用中，IDS的任务往往不仅在于检测，很多时候在IDS发现入侵行为以后，也需要IDS本身对入侵及时遏止。显然，要让处于旁路侦听的IDS完成这个任务又太难为，同时主链路又不能串接太多类似设备。在这种情况下，如果防火墙能和IDS、病毒检测等相关安全产品联合起来，充分发挥各自的长处，协同配合，共同建立一个有效的安全防范体系，那么系统网络的安全性就能得以明显提升。

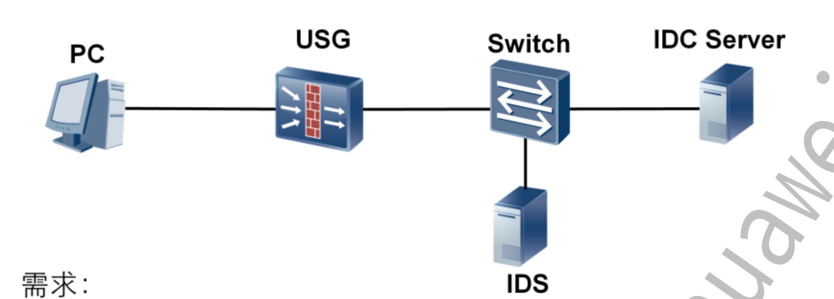
目前主要有两种解决办法：一种是直接把IDS、病毒检测部分直接“做”到防火墙中，使防火墙具有IDS和病毒检测设备的功能；另一种是各个产品分立，通过某种通讯方式形成一个整体，一旦发现安全事件，则立即通知防火墙，由防火墙完成过滤和报告。目前更看重后一种方案，因为它实现方式较前一种容易许多。

- **目前联动的IDS设备**
  - 可以和启明星辰的IDS联动；
  - 可以和安氏IDS联动；
  - 可以和天龙马IDS联动；
  - 可以和金诺网安IDS联动；
  - 支持与SIG联动功能；
  - 支持与NIP联动功能。




- 防火墙联动：
  - 配置防火墙和NIP来组成入侵防护方案；
  - 防火墙联动的响应流程：黑客入侵→通过防火墙进入网络→交换机镜像流量给NIP →黑客到达服务器→开始入侵→同时NIP得到镜像流量发现攻击行为记录入侵行为→ NIP联动防火墙→防火墙进行黑名单配置→黑客的入侵被阻断。

# 配置IDS联动举例




- 需求：
  - USG设备与IDS设备联合工作，共同保护内部网络安全。
  - USG设备与IDS服务器的认证方式和认证字分别为MD5和abcdef123。
  - USG设备与IDS服务器通过30000号端口进行通信。





# 配置IDS联动举例

- 配置IDS服务器IP地址。

```
[USG5000] firewall ids server 192.168.10.10 # 配置统一安全网关和IDS服务器通讯的端口号。
[USG5000] firewall ids port 30000 # 配置统一安全网关的报文认证方式和认证字。
[USG5000] firewall ids authentication type md5 key abcdef123
```

- 使能统一安全网关IDS联动功能。

```
[USG5000] firewall ids enable
```








统一安全网关上配置的IDS服务器的IP地址、端口号、认证方式和认证字需要与IDS服务器上的配置保持一致。



# 目录









# ARP攻击防范

- 攻击介绍
  - 攻击者通过发送大量伪造的ARP请求、应答报文攻击网络设备，主要有ARP缓冲区溢出攻击和ARP拒绝服务攻击两种。 ARP Flood攻击（ARP扫描攻击）：攻击者利用工具扫描本网段或者跨网段主机时，网络设备会查找ARP表项，如果目的IP地址的MAC地址不存在，那么必然会导致ARP模块向上层软件发送大量的ARP Miss消息 。
- 处理方法
  - 配置基于接口、区域或IP的ARP Flood攻击防范参数，限制接口上每秒ARP报文的总数。







# ARP flood攻击防范配置

- 防范配置

```
firewall defend arp-flood enable
```

- 配置ARP Flood攻击防范参数。

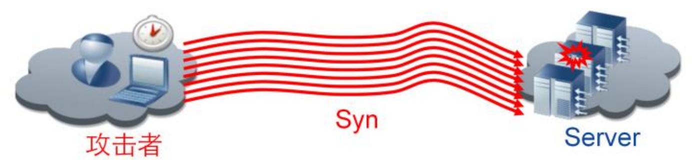
```
firewall defend arp-flood interface GigabitEthernet 1/0/0 max-rate 100
```






- max-rate的单位为包/秒

## SYN Flood攻击防范




- 攻击介绍
  - SYN Flood攻击就是采用源地址伪造的方式对目标主机发送大量的SYN报文，导致目标主机瘫痪。
- 处理方法
  - 采用TCP PROXY的方式进行SYN Flood攻击防御，其基本参数就是需要指定对那些主机进行保护；
  - 反向源探测技术；
  - 目标主机进行SYN报文限速的方式进行防御。

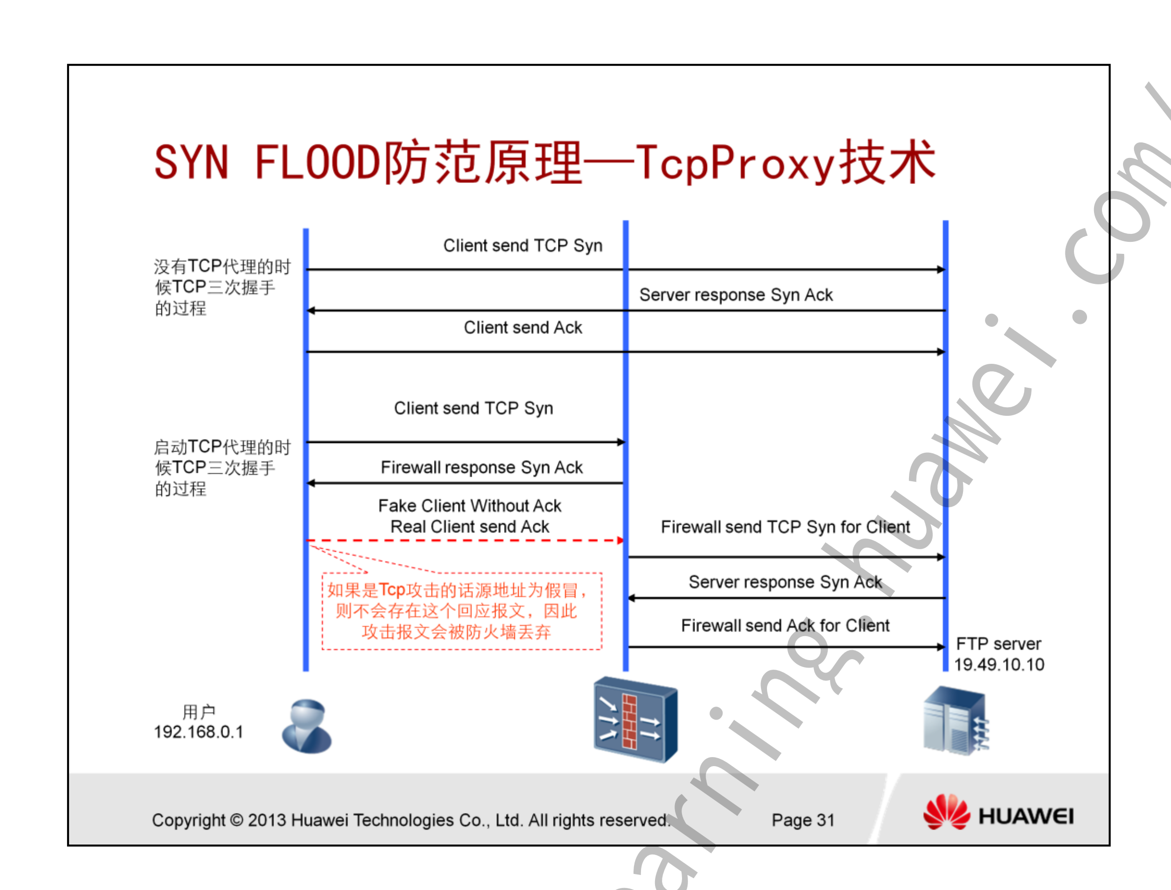




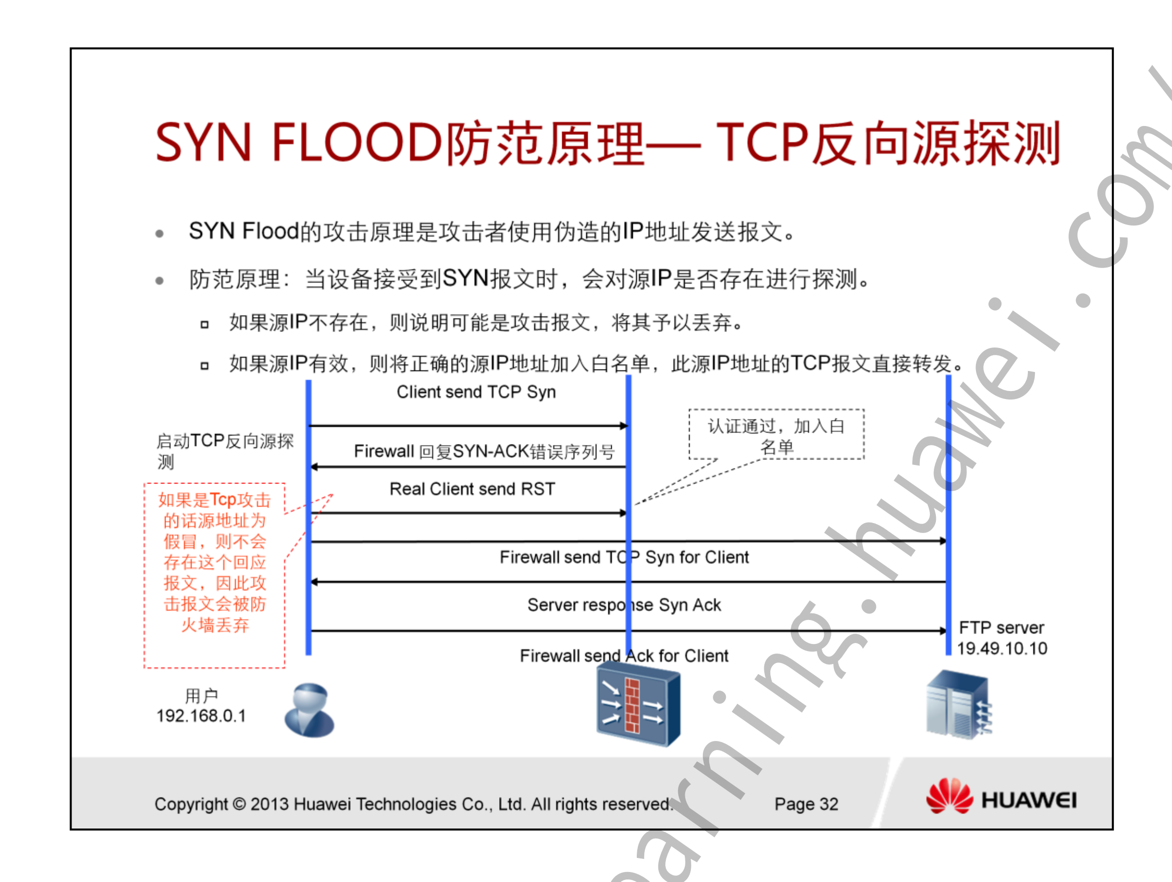

- 使用限制

无限制，但是需要区别SYN FLOOD和SYN报文扫描攻击，SYN FLOOD攻击的源地址是伪造的。而SYN报文扫描探测的源地址是真实的，而目的地址是按照一定规律变化的。

SYN FLOOD攻击和SYN报文扫描攻击的防御方法是不一样的。SYN报文扫描攻击可以加入黑名单，而SYN FLOOD攻击是不可能加入黑名单。




TCPProxy技术是进行Syn flood防御的关键技术。




由于反向源探测机制不受会话表是否成功建立的影响，所以推荐使用反向源探测技术来进行SYN Flood的攻击防范。如果必须使用TCP代理方式的攻击防范，则必须开启状态检测机制。

# SYN Flood攻击防范配置（一）

- 攻击防范配置
  - syn flood攻击防范开关

```
[USG] firewall defend syn-flood enable
```

  - 基于接口进行syn flood增强型攻击防范

```
[USG] firewall defend syn-flood interface all [max-rate rate-value] [tcp-proxy { auto | off | on }]
[USG] firewall defend syn-flood interface Ethernet slot-number [max-rate rate-value] [tcp-proxy { auto | off | on }]
[USG] firewall defend syn-flood interface GigabitEthernet slot-number [max-rate rate-value] [tcp-proxy { auto | off | on }]
[USG] firewall source-ip detect interface { interface-type interface-number | all } [ alert-rate alert-rate-number ] [ max-rate max-rate-number ]
firewall source-ip detect interface与firewall defend syn-flood interface可以同时配置。
```






- Syn flood攻击防范配置:

  [USG] firewall defend syn-flood enable　　// Syn flood攻击防范开关

  **注意:**

  关闭syn flood攻击防范功能，为undo firewall defend syn-flood enable；

  缺省允许通过的最大TCP报文速率是1000包/秒，自动启用TCP代理防范功能。缺省情况下，syn flood攻击防范功能是关闭的。

- 基于接口进行syn flood增强型攻击防范:

  其中：all，对于防火墙所有接口使能syn flood攻击防范。 rate-value，允许通过的TCP报文速率，取值范围为1～65535，缺省是1000，单位为包/秒。

  slot-number，接口的编号。 auto，自动启用TCP-PROXY防范功能，tcp-proxy缺省配置。off，不启用TCP-PROXY防范功能。on，直接启用TCP-PROXY防 范功能。

  **注意:**

  防火墙使能了增强型syn flood攻击防范，能够承受120万包/秒的攻击；

  对于**tcp-proxy**，指定为**auto**或**off**时，防火墙对于syn flood攻击防范是通过限制报文速率的方式实现，低于限制报文速率的报文还是会到达被攻击的设备。对于**tcp-proxy**，指定为**on**时，防火墙对每个TCP会话都会启用TCP-PROXY功能，攻击报文不会到达被攻击的设备；

  一般推荐的允许通过TCP报文速率是100包/秒。可以根据现场应用灵活改动。

# SYN Flood攻击防范配置（二）

- 攻击防范配置
  - 基于安全域进行syn flood攻击防范

[USG] firewall defend syn-flood zone zone-name [max-rate rate-value] [tcp-proxy { auto | off | on }]

zone-name：被保护安全区域名称；

rate-value：允许通过TCP报文速率，取值范围为1～65535，缺省是1000，单位为包/秒；

auto：自动启用TCP-PROXY防范功能，tcp-proxy缺省配置；

off：不启用TCP-PROXY防范功能；

on：直接启用TCP-PROXY防范功能。








- 基于安全域进行syn flood攻击防范

  [USG] **firewall defend syn-flood zone** *zone-name* [**max-rate** *rate-value*] [**tcp-proxy** { **auto** | **off** | **on** }]

  **注意：**

  关闭安全域syn flood攻击防范功能，为**undo firewall defend syn-flood zone** [*zone-name*]；

  该命令用于保护安全区域内所有的用户设备；

  对于**tcp-proxy**，指定为**auto**或**off**时，防火墙对于syn flood攻击防范是通过限制报文速率的方式实现，低于限制报文速率的报文还是会到达被攻击的设备；

  对于**tcp-proxy**，指定为**on**时，防火墙对每个TCP会话都会启用TCP-PROXY功能，攻击报文不会到达被攻击的设备。

  一般推荐的允许通过TCP报文速率是1000包/秒，可以根据现场应用灵活改动。

# SYN Flood攻击防范配置（四）

- 攻击防范配置举例

```
[USG] firewall defend syn-flood enable
[USG] firewall defend syn-flood zone trust tcp-proxy on
[USG] firewall defend syn-flood interface GigabitEthernet 1/0/0
tcp-proxy on
```





## Connection Flood攻击防范




- **攻击介绍**
  - 攻击者向被攻击服务器发送大量的请求，使被攻击服务器产生大量链接而不能受理合法用户的请求 。
- **处理方法**
  - USG统计用户向服务器发送的报文，如果在设定的时间间隔内用户发送的报文少于设定的阈值，则认为该用户不合法；
  - USG统计用户和服务器建立的链接数，如果在设定的时间间隔内用户建立的链接数大于设定的阈值，则认为该用户不合法；
  - USG将该IP地址加入黑名单。






与SYN Flood不同，TCP全连接攻击是指攻击者与被攻击对象正常建立了TCP全连接，但是却没有后续的报文，占用被攻击者的资源的攻击类型。通过配置防范功能，将TCP连接建立后不继续进行报文交互的连接作为不正常连接。当不正常连接超过阈值时，对其进行阻断。

## Connection Flood攻击防范配置

- 防范配置

```
firewall defend tcp-illeage-session enable
```

- 配置Connection Flood攻击防范参数

```
firewall defend tcp-illeage-session packet 1 interval 15
firewall defend tcp-illeage-session number 8  interval 15
firewall defend tcp-illeage-session blacklist-timeout 60
```








执行命令firewall defend tcp-illegal-session packet packet-number [ interval interval ]，设置阻断异常连接的标准。

当一条会话建立后，在设定的interval时间内，如果匹配该条会话的数据包数小于packet-number，则认为该会话为异常会话。

interval为可选参数，如果不配置，则按缺省值30秒计算。

执行命令firewall defend tcp-illegal-session number session-number [ interval interval ]，设置将攻击源加入黑名单，直接丢弃攻击源的所有报文的标准。

当某IP地址在interval时间内发起的异常会话数超过session-number后，设备认为该IP地址在进行全连接攻击，将该IP地址加入黑名单一段时间。

interval为可选参数，如果不配置，则按缺省值15秒计算。

执行命令firewall defend tcp-illegal-session blacklist-timeout time-out-value，配置将攻击者加入黑名单后老化时间。

当某个IP被加入到黑名单之后，需要经过老化时间之后，才会被从黑名单中删除，该IP才可以继续通信。

缺省情况下，将TCP全连接扫描攻击者加入黑名单的时间为20分钟，在这段时间里，攻击者发送的报文将被丢弃。用户也可以根据实际需求，调整黑名单老化时间。

# ICMP/UDP Flood攻击防范




- 攻击介绍
  - 短时间内向特定目标发送大量的UDP/ICMP报文，致使目标系统负担过重而不能处理合法的连接。
- 处理方法
  - 检测通向特定目的地址的UDP报文速率，当速度超过设定阈值上限时，设定攻击标志并做Car处理，对攻击记录日志。当速率低于设定的阈值下限，取消攻击标志，允许所有报文通向特定目的地址。




HUAWEI

- 使用限制

无使用限制，注意配置正确的目的保护地址。ICMP/UDP是无连接的协议，因此不能提供类似SYN FLOOD代理方式的防御方法。

# ICMP/UDP Flood攻击防范配置

- 防范配置

  Udp/Icmp Flood攻击防范配置步骤：

```
[USG] firewall defend udp-flood zone trust max-rate 3000
[USG] firewall defend icmp-flood interface GigabitEthernet 1/0/0 max-rate 500
[USG] firewall defend udp-flood interface GigabitEthernet 1/0/0 max-rate 1000
[USG] firewall defend udp-flood fingerprint-hit destination-max-rate 6
```








**firewall defend udp-flood fingerprint-hit** { **source-max-rate** [ *source-max-rate-value* ] | **destination-max-rate** [ *destination-max-rate-value* ] }

*source-max-rate-value* 指定一秒内基于源IP地址的UDP报文指纹匹配次数。

整数形式，取值范围为1～1024，单位为次。缺省值为3次。

*destination-max-rate-value* 指定一秒内基于目的IP地址的UDP报文指纹匹配次数。

整数形式，取值范围为1～1024，单位为次。缺省值为5次。

## HTTP Flood攻击攻击防范




- 攻击介绍
  - 攻击者直接或者间接向目标服务器发起大量的HTTP报文，导致服务器消耗过重，无法响应正常的请求，严重时会导致主干链路拥塞。
- 处理方法
  - 通过在接口对HTTP报文进行速率限制，实现HTTP Flood的攻击防范功能。
  - 针对HTTP Flood的防范可以设置重定向检测功能。将HTTP报文速率超过告警阈值的访问者重定向至一个虚拟页面。







HTTP Flood攻击是指攻击者直接或者间接向目标服务器发起大量的HTTP报文，导致服务器消耗过重，无法响应正常的请求，严重时会导致主干链路拥塞。通过在接口对HTTP报文进行速率限制，实现HTTP Flood的攻击防范功能。

设备的防范原理是对接收的HTTP报文速率进行限制，当接收的HTTP报文速率超过设定的阈值时，则视为攻击，并给予丢弃。

针对HTTP Flood的防范可以设置重定向检测功能。将HTTP报文速率超过告警阈值的访问者重定向至一个虚拟页面，如果访问者合法，它将做出合理回应，如果访问者非法则不会做回应。以此来判断HTTP报文的来源是否真实存在。

## HTTP Flood攻击防范配置

- 防范配置

  firewall defend http-flood enable

- 配置基于接口的HTTP Flood攻击防范参数

```
firewall defend http-flood source-detect interface { interface-type
interface-number | all } [ alert-rate alert-rate-number ] [ max-rate
max-rate-number ]
```






执行命令firewall defend http-flood enable，开启HTTP Flood攻击防范功能。

执行命令firewall defend http-flood source-detect interface { *interface-type interface-number* | all } [ alert-rate *alert-rate-number* ] [ max-rate *max-rate-number* ]，配置基于接口的HTTP Flood攻击防范参数。

**可选：**执行命令firewall source-ip detect aging-time *interval*，配置白名单老化时间。

重定向检测成功的IP地址会被加入到白名单，该IP地址发送的报文将在老化时间之内被直接转发，不再继续进行检测。缺省情况下，白名单的老化时间为1800秒。

# 流量型攻击Web配置



防火墙 安全防护 攻击防范
攻击防范配置列表
攻击防范类型
流量型
SYN Flood
UDP Flood
ICMP Flood
ARP Flood
应用层
SIP Flood
HTTP Flood
Connection Flood
扫描类
畸形报文类
特殊报文控制类
攻击报文处理方式
丢弃
应用
配置SYN Flood攻击防范
防范功能
启用
TCP最大报文段长度
1460
<100-1460>字节
基于源探测（推荐配置）
基于TCP代理（可选配置）
新建 删除 刷新 全局设置
接口
配置
没有记录
①选择相应的攻击防范类型
②启用对应的功能，设置全局参数
③设置具体的参数



# 目录









## 地址扫描攻击防范

- 攻击介绍
  - 运用ping程序探测目标地址，以用来确定目标系统是否存活的标识。也可使用TCP/UDP报文对目标系统发起探测（如TCP ping）。
- 处理方法
  - 检测进入防火墙的ICMP、TCP和UDP报文，由该报文的源IP地址获取统计表项的索引，如目的IP地址与前一报文的IP地址不同，则将表项中的总报文个数增1。如在一定时间内报文的个数达到设置的阈值，记录日志，并根据配置决定是否将源IP地址自动加入黑名单。
- 攻防配置

```
[USG] firewall zone untrust
[USG-zone-untrust] statistic enable ip outzone
[USG] firewall defend ip-sweep max-rate 1000
[USG] firewall defend ip-sweep blacklist-timeout 5
[USG] firewall defend ip-sweep enable
```






- **使用限制**

扫描类攻击的源地址是真实的，因此可以采用直接加入黑名单的方法进行防御。扫描类攻击的扫描速度决定了攻击防范的有效性。蠕虫病毒爆发的时候，伴随者一般就是地址扫描攻击。

【命令】

**firewall defend ip-sweep** { **max-rate** *rate-number* | **blacklist-timeout** *interval* | **enable** }

**undo firewall defend ip-sweep** { **max-rate** | **blacklist-timeout** | **enable** }

【参数】

**max-rate** *rate-number*：设定从同一源地址向外发送报文的目的地址变化速率的阈值。*rate-number* 默认值为4000 包/秒，取值范围为1 包/秒～10,000 包/秒。

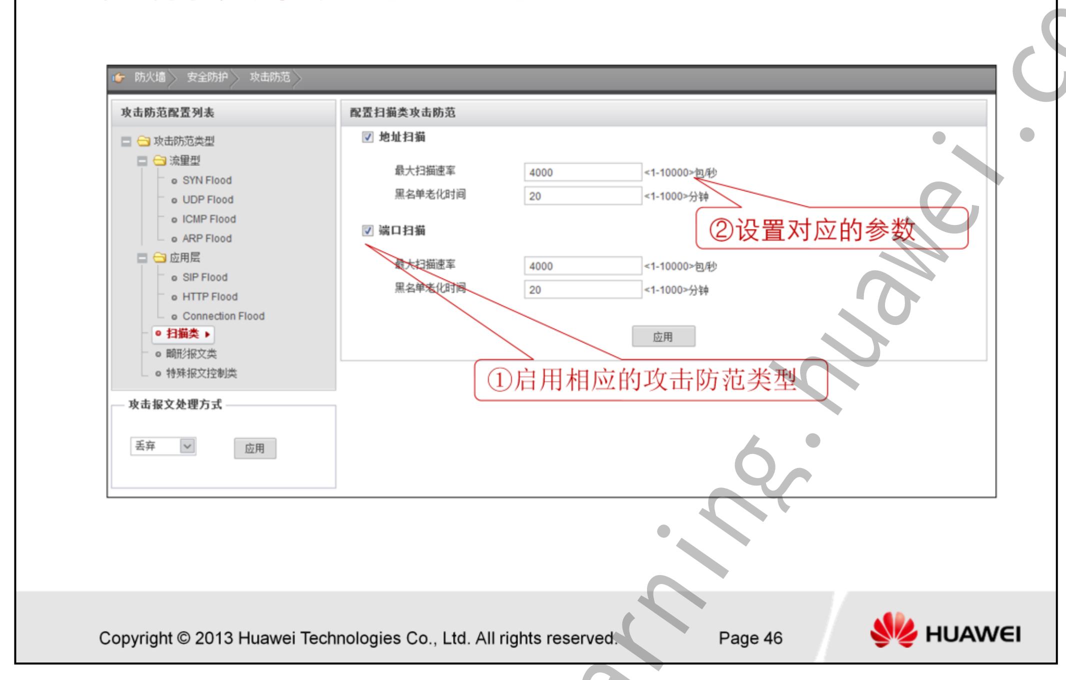
**blacklist-timeout** *interval*：将攻击源IP 加入黑名单并设定其在黑名单内的保持时间，*interval* 取值范围为1min～1000min，默认值为0min，即不加入黑名单。

**enable**：使能地址扫描攻击防范功能开关。

【举例】

# 打开地址扫描攻击防范功能开关，设定扫描速率的阈值为1000。

```
[USG] firewall defend ip-sweep max-rate 1000
```


扫描窥探攻击Web配置
防火墙 安全防护 攻击防范
攻击防范配置列表
攻击防范类型
流量型
SYN Flood
UDP Flood
ICMP Flood
ARP Flood
应用层
SIP Flood
HTTP Flood
Connection Flood
扫描类
畸形报文类
特殊报文控制类
攻击报文处理方式
丢弃
应用
配置扫描类攻击防范
地址扫描
最大扫描速率 4000 <1-10000>包/秒
黑名单老化时间 20 <1-1000>分钟
端口扫描
最大扫描速率 4000 <1-10000>包/秒
黑名单老化时间 20 <1-1000>分钟
应用
②设置对应的参数
①启用相应的攻击防范类型
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 46
HUAWEI

# 端口扫描攻击防范

- 攻击介绍
  - Port Scan攻击通常使用一些软件，向大范围的主机的一系列TCP/UDP端口发起连接，根据应答报文判断主机是否使用这些端口提供服务。
- 处理方法
  - 检测进入防火墙的TCP报文或UDP报文，由该报文的源IP地址获取统计表项的索引，如目的端口与前一报文不同，将表项中的报文个数增1。如果报文的个数超过设置的阈值，记录日志，并根据配置决定是否将源IP地址加入黑名单。
- 攻防配置

```
[USG] firewall zone untrust
[USG-zone-untrust] statistic enable ip outzone
[USG] firewall defend port-scan max-rate 1000
[USG] firewall defend port-scan blacklist-timeout 5
[USG] firewall defend port-scan enable
```








- 【命令】

firewall defend port-scan { max-rate *rate-number* | blacklist-timeout *interval* | enable }

undo firewall defend port-scan { max-rate | blacklist-timeout | enable }

【参数】

max-rate *rate-number*：设定从同一源地址向外发送报文的目的端口变化速率的阈值。*rate-number*默认值为4000 次/秒，取值范围为1 次/秒～10,000 次/秒。

blacklist-timeout *interval*：将攻击源IP 加入黑名单并设定其在黑名单内的保持时间，*interval*取值范围为1min～1000min，默认值为0min，即不加入黑名单。

enable：使能端口扫描攻击防范功能开关。

【举例】

# 打开端口扫描攻击防范功能开关，设定扫描速率的阈值为1000。

<USG> system-view

[USG] firewall defend port-scan enable

[USG] firewall defend port-scan max-rate 1000



# 目录

1. 网络攻击介绍
2. 防火墙攻击防范通用技术
3. 防火墙攻击防范应用分析

   3.1 流量型攻击

   3.2 扫描窥探攻击

   **3.3 畸形报文攻击**

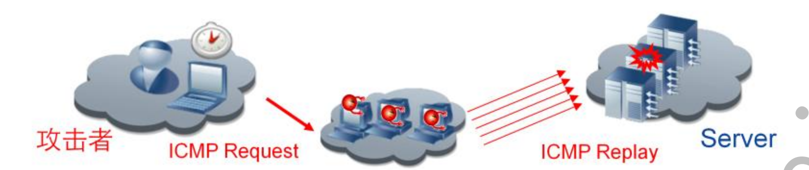
   3.4 特殊报文攻击

   3.5 其他攻击






## SMURF攻击防范




- 攻击介绍
  - Smurf攻击方法是发ICMP请求，该请求包的目标地址设置为受害网络的广播地址，这样该网络的所有主机都对此ICMP应答请求作出答复，导致网络阻塞。
- 处理方法
  - 检查ICMP应答请求包的目的地址是否为子网广播地址或子网的网络地址，如是，则直接拒绝，并将攻击记录到日志。
- 攻防配置

```
firewall defend smurf enable
```





Smurf攻击方法是发ICMP应答请求，该请求包的目标地址设置为受害网络的广播地址，这样该网络的所有主机都对此ICMP应答请求作出答复，导致网络阻塞。高级的Smurf攻击，主要用来攻击目标主机。方法是将上述ICMP应答请求包的源地址改为受害主机的地址，最终导致受害主机雪崩。

使用限制

由于路由器等三层设备本身就不会转发目的地址是广播地址的报文，因此SMURF攻击在网络上很难形成攻击。在防火墙上，检查SMURF攻击必须要求被攻击网络是直接连接到防火墙上。

# LAND攻击防范




- 攻击介绍
  - 把TCP 的源地址和目标地址都设置成某一个受害者的IP地址。这将导致受害者向它自己的地址发送SYN-ACK消息，结果这个地址又发回ACK消息并创建一个空连接，占用系统资源或使目的主机崩溃。
- 处理方法
  - 对每一个的IP报文进行检测，若其源地址与目的地址相同，或者源地址为环回地址(127.0.0.1)，则直接拒绝，并将攻击记录到日志。
- 攻防配置

```
firewall defend land enable
```






所谓Land攻击，就是把TCP SYN包的源地址和目标地址都设置成某一个受害者的IP地址。这将导致受害者向它自己的地址发送SYN-ACK消息，结果这个地址又发回ACK消息并创建一个空连接，每一个这样的连接都将保留直到超时掉。各种受害者对Land攻击反应不同，许多UNIX主机将崩溃，NT主机会变的极其缓慢。

使用限制：没有限制，对性能也基本无影响，对网络也不会造成不良影响。

## Fraggle攻击防范

- 攻击介绍
  - Fraggle类似于Smurf攻击，使用UDP应答消息而非ICMP。UDP端口7(ECHO)和端口19(Chargen)在收到UDP报文后，大量无用的应答报文，占满网络带宽。
- 处理方法
  - 检查进入防火墙的UDP报文，若目的端口号为7或19，则直接拒绝，并将攻 击记录到日志，否则允许通过。
- 攻防配置

```
firewall defend fraggle enable
```






Fraggle类似于Smurf攻击，只是使用UDP应答消息而非ICMP。UDP端口7（ECHO）和端口19（Chargen）在收到UDP报文后，都会产生回应。在UDP的7号端口收到报文后，会回应收到的内容，而UDP的19号端口在收到报文后，会产生一串字符流。它们都同ICMP一样，会产生大量无用的应答报文，占满网络带宽。 攻击者可以向子网广播地址发送源地址为受害网络或受害主机的UDP包，端口号用7或19。子网络启用了此功能的每个系统都会向受害者的主机作出响应，从而引发大量的包，导致受害网络的阻塞或受害主机的崩溃；子网上没有启动这些功能的系统将产生一个ICMP不可达消息，因而仍然消耗带宽。 也可将源端口改为Chargen，目的端口为ECHO，这样会自动不停地产生回应报文，其危害性更大。

## IP Fragment攻击

- 攻击介绍
  - IP报文中有几个字段与分片有关：DF位、MF位，Fragment Offset 、Length 。如果上述字段的值出现矛盾，而设备处理不当，会对设备造成一定的影响，甚至瘫痪。
- 处理方法
  - 检查IP报文中与分片有关的字段（DF位、MF位、片偏置量、总长度）是否以下矛盾，如发现含有如下矛盾，则直接丢弃。将攻击记录到日志：
    - DF位为1，而MF位也为1或Fragment Offset不为0；
    - DF位为0，而Fragment Offset + Length > 65535。
- 攻防配置

```
[USG]firewall defend ip-fragment enable
```






- **攻击介绍**

IP报文中有几个字段与分片有关：DF位、MF位，Fragment Offset 、Length 。

如果上述字段值出现矛盾，而设备处理不当，会对设备造成一定的影响，甚至瘫痪。

矛盾的情况有：

DF位被置位，而MF位同时被置位或Fragment Offset不为0；

DF位为0，而Fragment Offset + Length > 65535。

- **处理方法**

若分片报文的目的地址为本防火墙，则直接丢弃；

检查IP报文中与分片有关的字段（DF位、MF位、片偏置量、总长度）是否以下矛盾：

DF位为1，而MF位也为1或Fragment Offset不为0；

DF位为0，而Fragment Offset + Length > 65535。

如发现含有（1）或（2）错误的IP分片报文，则直接丢弃。将攻击记录日志。

## IP spoofing攻击防范

- 攻击介绍
  - 为了获得访问权，或隐藏入侵者的身份信息，入侵者生成带有伪造源地址的报文。
- 处理方法
  - 检测每个接口流入的IP报文的源地址与目的地址，并对报文的源地址反查路由表，入接口与以该IP地址为目的地址的最佳出接口不相同的IP报文被视为IP Spoofing攻击，将被拒绝，并进行日志记录。
- 攻防配置

```
firewall defend ip-spoofing enable
```






- IP Spoof

攻击介绍：为了获得访问权，入侵者生成一个带有伪造源地址的报文。对于使用基于IP地址验证的应用来说，此攻击方法可以导致未被授权的用户可以访问目的系统，甚至是以root权限来访问。即使响应报文不能达到攻击者，同样也会造成对被攻击对象的破坏。这就造成IP Spoofing攻击。

# Ping of Death攻击

- 攻击介绍
  - IP报文的长度字段为16位，这表明一个IP报文的最大长度为65535。Ping of Death，利用一些尺寸超大的ICMP报文对系统进行的一种攻击。
- 处理方法
  - 检测ICMP请求报文长度是否超过65535KB，若超过丢弃报文并记录日志。
- 攻防配置

```
[USG] firewall defend ping-of-death enable
```

IP PINGDATA
20 8 1472
Flag MF
Offset 0

IP DATA
20 1480
Flag MF
Offset 1480

IP DATA
20 1480
Flag MF
Offset 2960

IP DATA
20 1480
Flag MF
Offset 4440

IP DATA
20 1480
Flag MF
Offset 65120

20 568
Flag Last Fragment
Offset 66600







Ping of Death：对于ICMP ECHO Request报文，如果数据长度大于65508，就会使ICMP数据＋IP头长度(20)＋ICMP头长度（8）＞65535。对于有些路由器或系统，在接收到一个这样的报文后，由于处理不当，会造成系统崩溃、死机或重启。

特征：ping报文全长超过65535；

目的：使被攻击设备因处理不当而死机；

配置：firewall defend ping-of-death enable；

原理：检查报文长度如果最后分片偏移量和本身长度相加超过65535，丢弃该分片。

## TCP Flag攻击

- 攻击介绍
  - TCP报文包含6个标志位：URG、ACK、PSH、RST、SYN、FIN ，不同的系统对这些标志位组合的应答是不同的，可用于操作系统探测。
- 处理方法
  - 处理方法：检查TCP报文的各个标志位，若出现
    - 6个标志位全为1或6个标志位全为0；
    - SYN和FIN位同时为1；syn和rst同时为1；fin和urg同时为1；rst和fin同时为1；
    - 直接丢弃满足以上任一条件的报文，并记录日志。
- 攻防配置

```
[USG]firewall defend tcp-flag enable
```








- 攻击介绍

TCP报文包含6个标志位：URG、ACK、PSH、RST、SYN、FIN ，不同的系统对这些标志位组合的应答是不同的：6个标志全部为1，也就是圣诞树攻击；6个标志全部为0，如果端口是关闭的，会使接收方应答一个RST | ACK消息。而对于一个开放端口，Linux和UNIX机器不会应答，而Windows机器将回答RST | ACK消息。这可用于操作系统探测。

不管端口是打开还是关闭，ACK与除RST外的其它任何一个状态位组合在一起，都会引起一个还没有发送请求的接收方的一个RST应答，这可用于探测主机的存在。不管端口是打开还是关闭，SYN | FIN | URG 会让接收方发送一个 RST | ACK 应答，这可用于探测主机的存在。

处理方法

检查TCP报文的各个标志位，若出现：

6个标志位全为1；

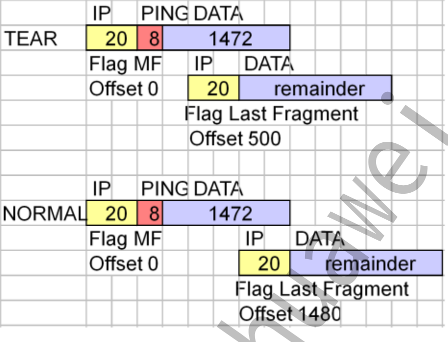
6个标志位全为0；

SYN和FIN位同时为1；

直接丢弃满足以上任一条件的报文，并记录日志。

# Tear Drop攻击

- 攻击介绍
  - Teardrop攻击利用在TCP/IP堆栈中信任IP碎片报文头所包含的信息来实现攻击。IP报文通过MF位、Offset字段、Length字段指示该分段所包含是原包哪一段信息，某些TCP/IP在收到含有重叠偏移伪造分段时将崩溃。




- 处理方法
  - 缓存分片信息，每一个源地址、目的地址、分片ID相同的为一组，最大支持缓存10000组分片信息。在分片缓存的组数达到最大时，如果后续分片报文要求建立新组，则直接丢弃。
- 攻防配置

```
[USG]firewall defend teardrop enable
```







- **攻击介绍**

Teardrop攻击利用那些在TCP/IP堆栈实现中信任IP碎片中的报文头所包含的信息来实现自己的攻击。IP报文中通过MF位、Offset字段、Length字段指示该分段所包含的是原包的哪一段的信息，某些TCP/IP在收到含有重叠偏移的伪造分段时将崩溃。

- **处理方法**

缓存分片信息，每一个源地址、目的地址、分片ID相同的为一组，最大支持缓存10000组分片信息。在分片缓存的组数达到最大时，如果后续分片报文要求建立新组，则直接丢弃。

# WinNuke攻击防范

- 攻击介绍
  - WinNuke攻击通常向装有Windows系统的特定目标的NetBIOS端口（139）发送OOB（out-of-band）数据包，引起一个NetBIOS片断重叠，致使已与其他主机建立连接的目标主机崩溃。还有一种是IGMP分片报文，一般情况下，IGMP报文是不会分片的，所以，不少系统对IGMP分片报文的处理有问题。
- 处理方法
  - WinNuke攻击1 检测数据包目的端口是否为139，并且检查TCP-URG位是否被设置；
  - WinNuke攻击2 检测进入的IGMP报文是否为分片报文，如是分片报文，则直接丢弃。
- 攻防配置

```
firewall defend winnuke enable
```







WinNuke攻击通常向装有Windows系统的特定目标的NetBIOS端口（139）发送OOB（out-of-band）数据包，引起一个NetBIOS片断重叠，致使已与其他主机建立连接的目标主机崩溃。还有一种是IGMP分片报文，一般情况下，IGMP报文是不会分片的，所以，不少系统对IGMP分片报文的处理有问题。如果收到IGMP分片报文，则基本可判定受到了攻击。

# 扫描窥探攻击Web配置

防火墙 > 安全防护 > 攻击防范

攻击防范配置列表

- 攻击防范类型
  - 流量型
    - SYN Flood
    - UDP Flood
    - ICMP Flood
    - ARP Flood
  - 应用层
    - SIP Flood
    - HTTP Flood
    - Connection Flood
  - 扫描类
  - 畸形报文类
  - 特殊报文控制类

攻击报文处理方式

丢弃 应用

配置畸形报文类攻击防范

防范功能 全部启用

- IP欺骗攻击防范
- Teardrop攻击防范
- Ping of Death攻击防范
- WinNuke攻击防范
- TCP报文标志合法性检测
- UDP短头报文攻击防范
- IP分片报文检测
- Smurf攻击防范
- Fraggle攻击防范
- Land攻击防范
- ARP欺骗攻击防范

应用

①启用相应的攻击防范类型



# 目录









## 超大ICMP报文攻击防范

- 攻击介绍
  - 超大ICMP报文攻击是指利用长度超大的ICMP报文对目标系统进行攻击。对于有些系统，在接收到超大ICMP报文后，由于处理不当，会造成系统崩溃、死机或重启。
- 处理方法
  - 用户可以根据实际网络需要配置允许通过的ICMP报文的最大长度，当实际ICMP报文的长度超过该值时，防火墙认为发生了超大ICMP报文攻击，将丢弃该报文。
- 攻防配置

```
firewall defend large-icmp enable
firewall defend large-icmp max-length [ length ]
```







- 配置步骤：

在用户视图下执行命令system-view，进入系统视图。

执行命令firewall defend large-icmp enable，开启超大ICMP报文攻击防范功能。

执行命令firewall defend large-icmp max-length [ length ]，配置超大ICMP报文攻击防范参数。如果没有指定length参数，缺省值为4000字节。

# ICMP不可达报文攻击防范

- 攻击介绍
  - 不同的系统对ICMP不可达报文的处理方式不同，有的系统在收到网络或主机不可达的ICMP报文后，对于后续发往此目的地址的报文直接认为不可达，从而切断了目的地与主机的连接。攻击者利用这一点，伪造不可 达ICMP报文，切断受害者与目的地的连接，造成攻击。
- 处理方法
  - 启动ICMP不可达报文攻击防范功能，防火墙对ICMP不可达报文进行丢弃并记录攻击日志。
- 攻防配置

```
firewall defend icmp-unreachable enable
```








- 配置步骤:

在用户视图下执行命令system-view，进入系统视图。

执行命令firewall defend icmp-unreachable enable，开启ICMP不可达报文攻击防范功能。

# Tracert报文攻击防范

- 攻击介绍
  - Tracert报文攻击是攻击者利用TTL为0时返回的ICMP超时报文，和达到目的地址时返回的ICMP端口不可达报文来发现报文到达目的地所经过的路径，它可以窥探网络的结构。
- 处理方法
  - 配置Tracert报文攻击防范就是对于检测到的超时的ICMP报文或UDP报文，或者目的端口不可达报文，给予丢弃。
- 攻防配置

```
firewall defend tracert enable
```








- 配置步骤:

  在用户视图下执行命令system-view，进入系统视图。

  执行命令firewall defend tracert enable，开启Tracert报文攻击防范功能。

# 特殊报文攻击攻击Web配置








HUAWEI



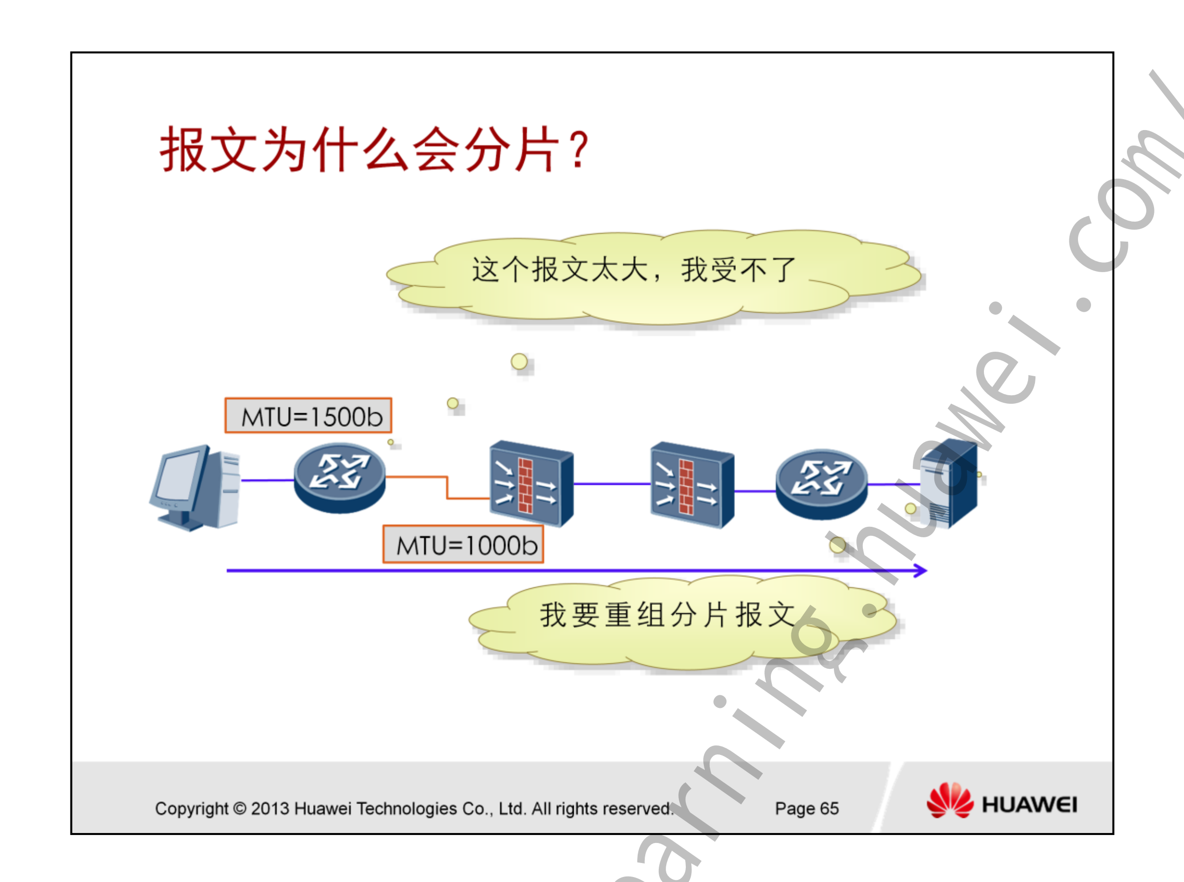
# 目录



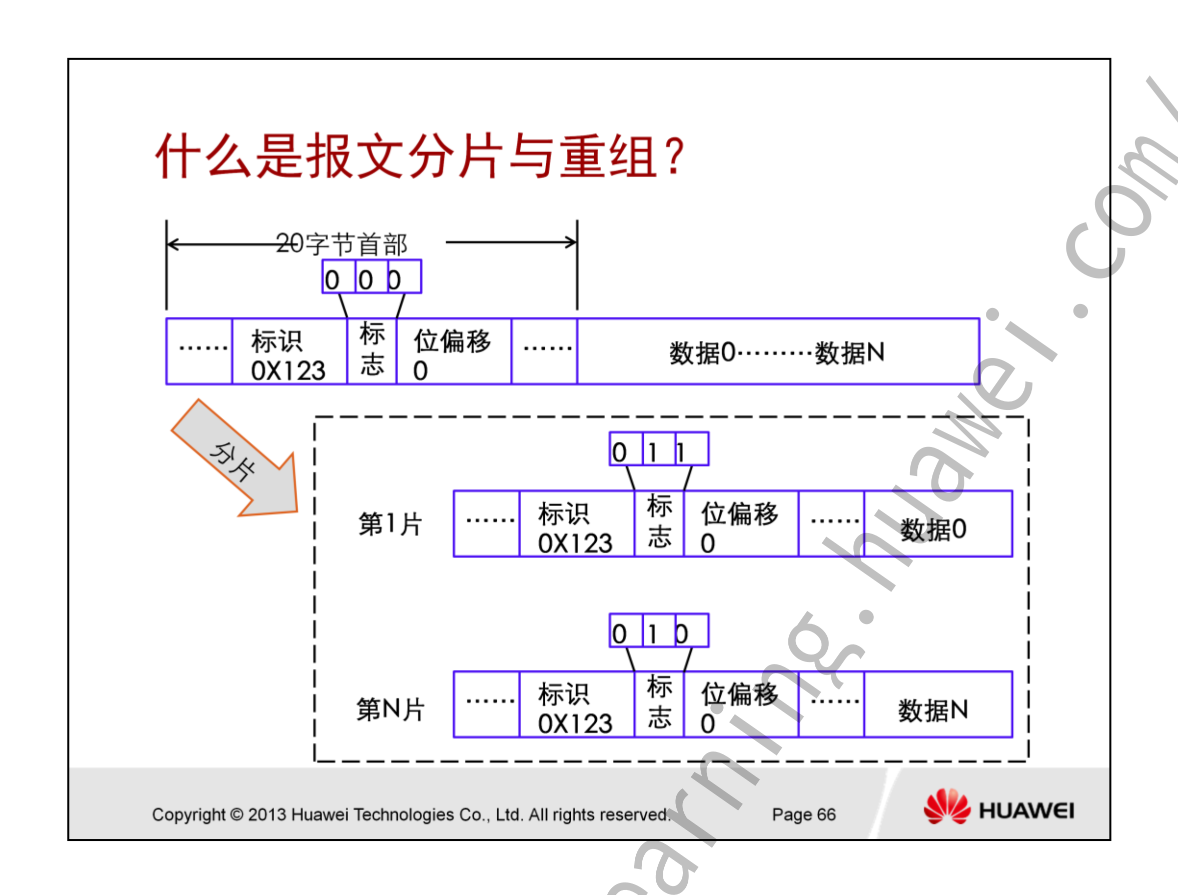




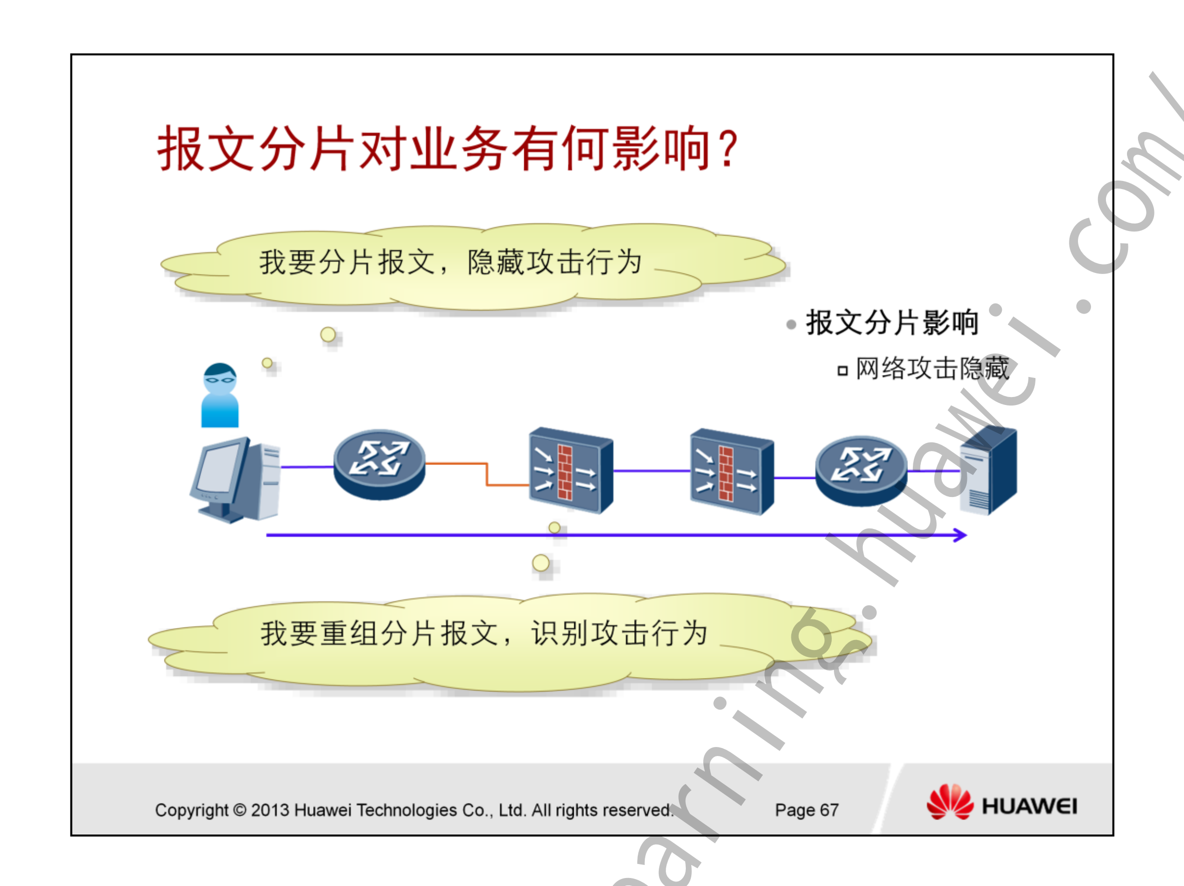





- 一条链路所能传输的最大报文长度被称为MTU（Maximum Transfer Unit，最大传输单元）。MTU通常与接口类型有关，一个报文在网络中传输可能会通过多种不同链路，如果报文长度比较大的话，超过了其中某条链路的MTU而无法通过该条链路，将会把报文分割到适合本链路MTU大小的多个报文，这个被分割之后的报文被称为分片报文；
- 理想的情况下，各分片报文按照固定的先后顺序在网络中传输，当目标设备接收到所有分片报文后再将这些报文重组为一个完整的报文。

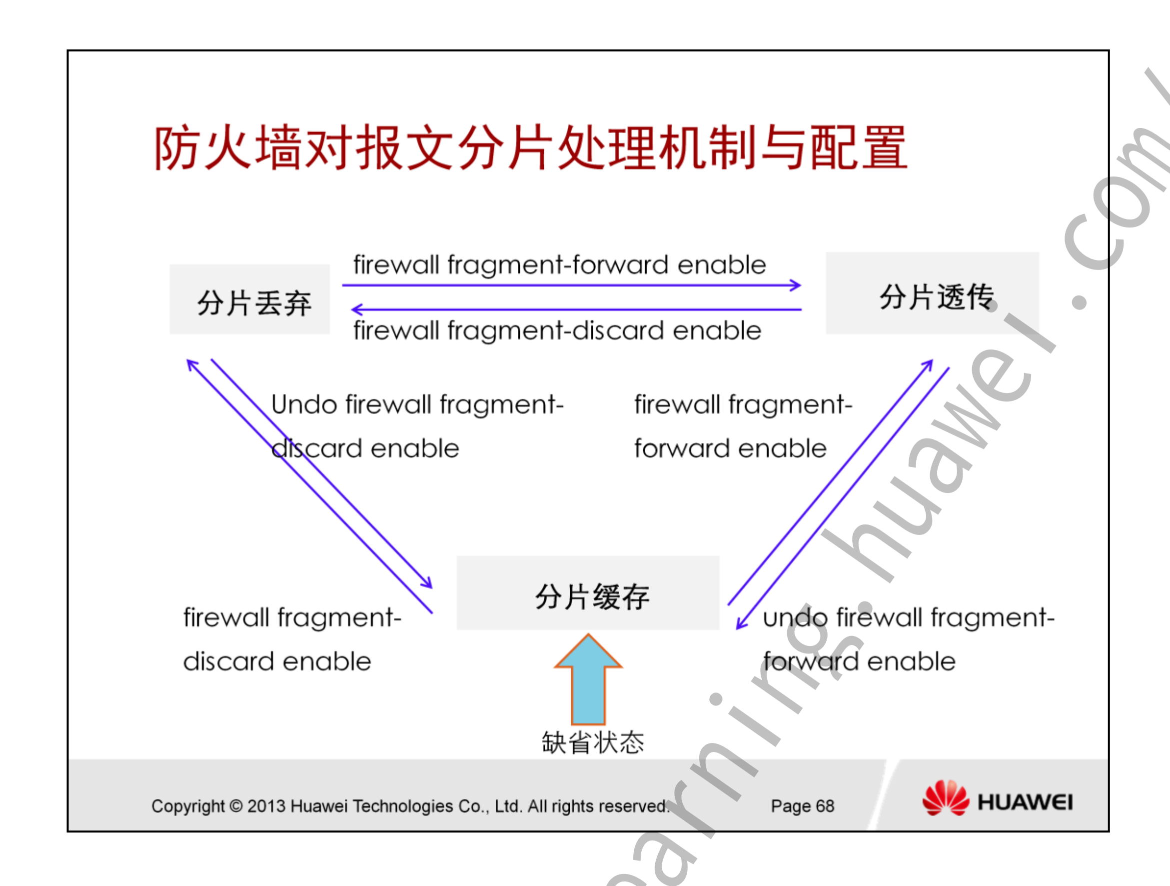



- 报文分片后，通过IP报文首部中的标识字段识别哪些分片是属于同一个报文的，通过片偏移字段记录该分片在整个报文中的位置，标志字段用最后一个比特来表示“更多分片”。除了最后一个分片外，其他每个组成数据报的分片都要把该比特置1；
- 一个网络设备在收到所有分片报文之后，就可以根据标识字段和片偏移字段来将所有分片重组为所有原来的完整报文。




- 由于分片报文的特殊性，分片报文经常会被利用来做网络攻击。同时分片报文的传输也经常因为某个分片的丢失而导致整个报文重传。所以在实际应用中，应尽量避免分片报文的出现。除了被非法用户作为网络攻击，分片报文对象VPN应用(主要指IPSEC和GRE)也会造成影响。

- 由于需要设备对分片报文进行重组后解密或者解封装，设备才能进行后续处理，所以必须将设备配置成分片缓存状态，完成原始报文重组之后，才可以进行相应的加密解密处理。在NAT应用中，需要设备对分片报文进行重组后才能正常解析和转换报文中的IP地址，所以也必须将设备配置成分片缓存状态，才可以正常进行NAT。在VPN应用中(主要指IPSEC和GRE)，由于需要设备对分片报文进行重组后解密或者解封装，设备才能进行后续处理，所以必须将设备配置成分片缓存状态，完成原始报文重组之后，才可以进行相应的加密解密处理。

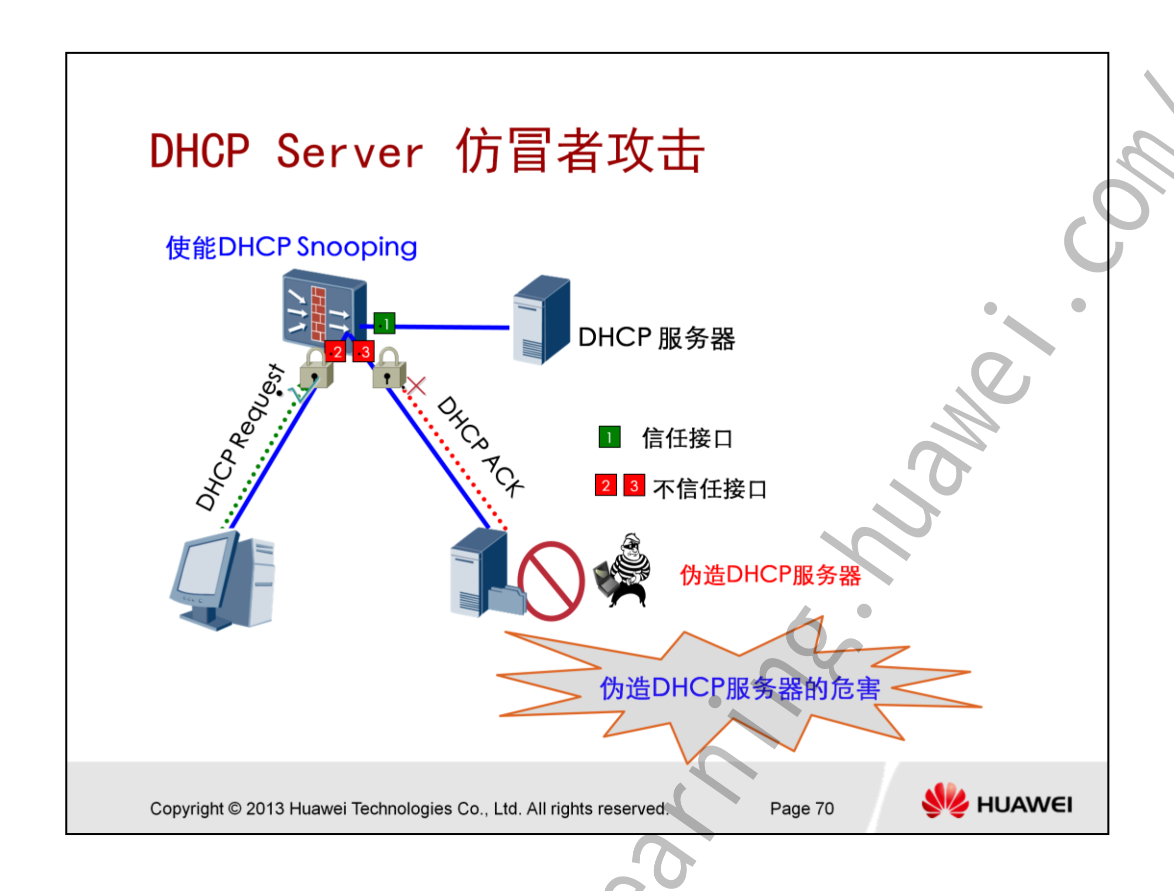



- 在实际传输过程中，由于网络环境的复杂，可能存在以下情况：
  - 后续分片报文先于首片报文到达某个网络设备；
  - 后续报文需要在某个中间设备上进行重组后才能继续传输，例如中间设备需要解析报文载荷后才能判断如何转发。
- 在USG上，这两种情况都可能存在设备上对分片报文的处理分为三种机制：
  - 分片缓存：设备缺省机制。设备会将非首片的分片报文缓存至分片散列表，等待首片到来建立会话后，将所有分片报文进行转发；
  - 分片丢弃：不信任所有分片报文，收到分片报文即丢弃。可以提供最大的安全性，但是可能会影响正常业务的转发；
  - 分片透传：信任所有分片报文，收到分片立即直接转发，不会缓存到分片散列表等待首包的到来。



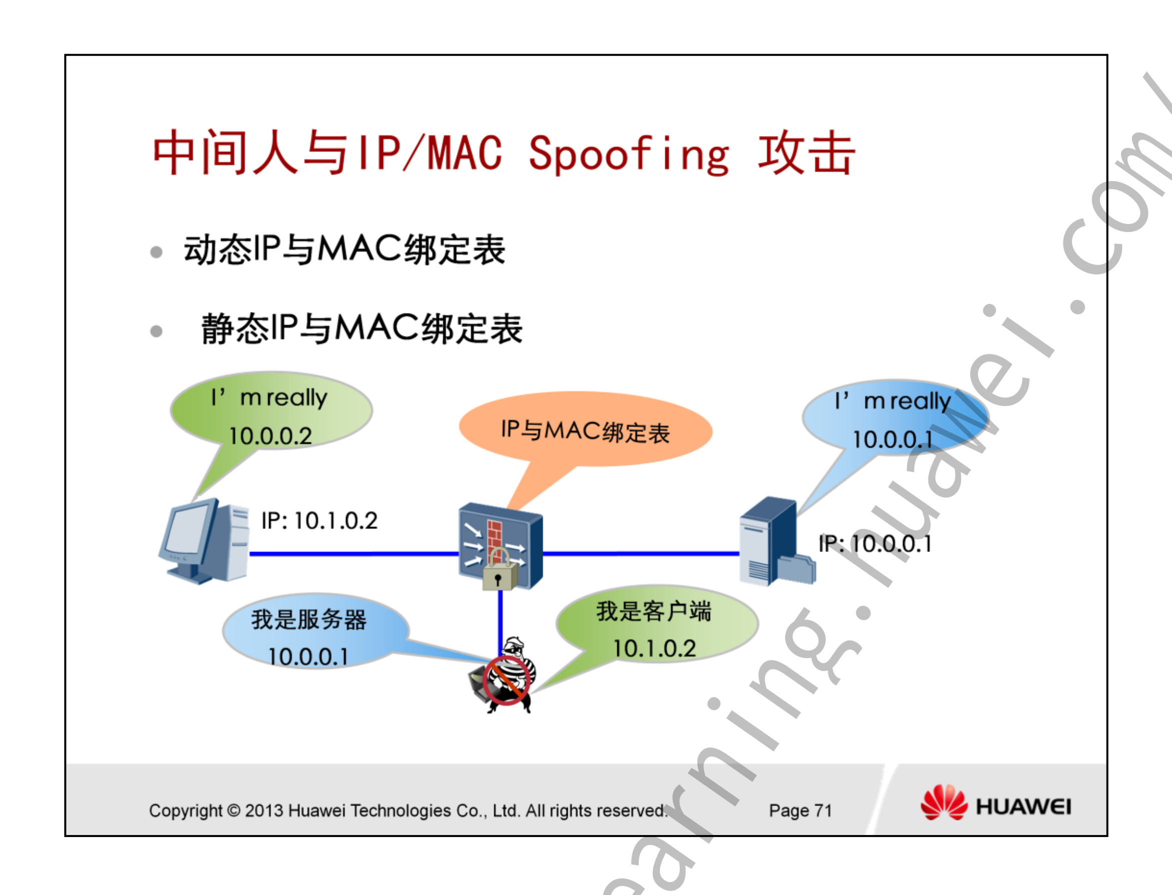

- 利用DHCP报文进行的攻击有多种类型，了解其攻击原理和通过DHCP Snooping技术进行防范的原理，有助于选择配置以下各种类型的攻击防范。

- DHCP Snooping是一种DHCP安全特性，通过MAC地址限制，DHCP Snooping安全绑定、IP + MAC绑定、Option82特性等功能过滤不信任的DHCP消息，解决了设备应用DHCP时遇到DHCP DoS攻击、DHCP Server仿冒攻击、ARP中间人攻击及IP/MAC Spoofing攻击的问题。DHCP Snooping的作用就如同在Client和DHCP Server之间建立的一道防火墙。




**应用场景**：当用户网络中存在DHCP Server 仿冒者时，DHCP Server 仿冒者回应给DHCP Client 仿冒信息，如错误的网关地址、错误的DNS 服务器、错误的IP 地址等，从而使DHCP Client 无法访问网络。

**防范思路**：为了避免受到DHCP Server仿冒者的攻击，可以在设备上配置DHCP Snooping功能，把用户侧的接口配置为Untrusted模式，把DHCP Server侧的接口配置为Trusted模式，所有从Untrusted接口收到的DHCP reply报文全部丢弃。



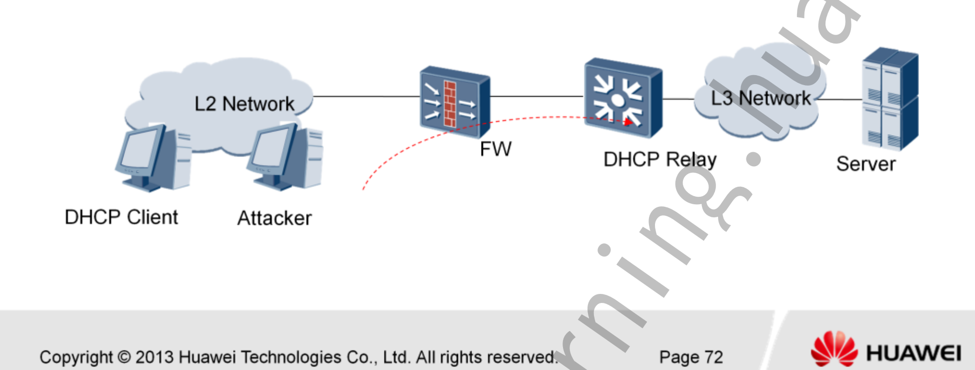

中间人攻击是指攻击者同时伪装为DHCP Server和Client，进行正常Server和Client之间报文的中转，从而获得用户数据的攻击。

**应用场景**：当网络中存在中间人或者IP/MAC Spoofing 攻击时，攻击者仿冒Server和Client，在服务器看来，所有的报文都是来自或者发往客户端；在客户端看来，所有的报文也都是来自或者发往服务器端。但实际上这些报文都是经过了中间人的“二手”信息。这样仿冒者就可以获得Server和Client的数据。

**防范原理**：为了避免受到中间人或IP/MAC Spoofing 攻击，可以在防火墙 上配置DHCP Snooping功能，使用DHCP Snooping 绑定功能，只有接收到的报文的信息和绑定表中的内容一致才会被转发，否则报文将被丢弃。

# 改变CHADDR 值的DoS 攻击

- CHADDR：Client Hardware Address；
- 攻击者改变的不是数据帧头部的源MAC 地址，而是改变DHCP 报文中的CHADDR；
- 检查DHCP Request 报文中CHADDR 字段。



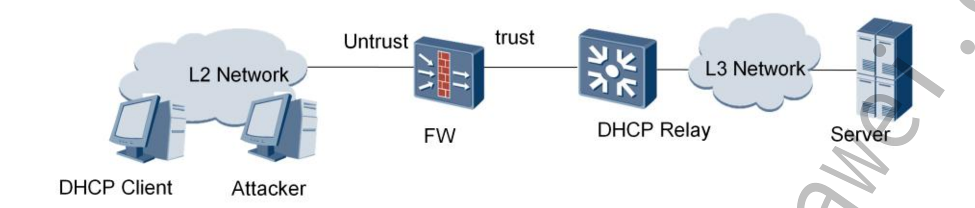





- 应用场景：当网络中存在DHCP饿死攻击时，攻击者改变的不是数据帧头部的源MAC，而是改变DHCP报文中的CHADDR（Client Hardware Address）值来不断申请IP地址。如果路由设备仅根据数据帧头部的源MAC来判断该报文是否合法，那么“MAC地址限制”方案不能完全起作用，这样的攻击报文还是可以被正常转发。

- 防范原理：为了避免受到攻击者改变CHADDR值的攻击，可以在设备上配置DHCP Snooping功能，检查DHCP Request报文中CHADDR字段。如果该字段跟数据帧头部的源MAC相匹配，便转发报文；否则，丢弃报文。

# Option82（仿冒DHCP续租报文攻击）




- 应用场景：当网络中存在攻击者时，攻击者通过不断发送DHCP Request报文来冒充用户续租IP。
- 防范原理：可以在设备上配置DHCP Snooping功能，检查DHCP Request报文和使用DHCP Snooping绑定功能.






- 应用场景：当网络中存在攻击者时，攻击者通过不断发送DHCP Request报文来冒充用户续租IP地址，这样一方面会导致一些到期的IP地址无法正常回收，另外也不是用户的真实意图。

- 防范原理：为了避免受到攻击者仿冒DHCP续租报文进行攻击，可以在设备上配置DHCP Snooping功能，检查DHCP Request报文和使用DHCP Snooping绑定功能，只有接收到的报文的信息和绑定表中的内容一致才会被认为是正常的申请报文，报文被转发，否则报文将被丢弃。

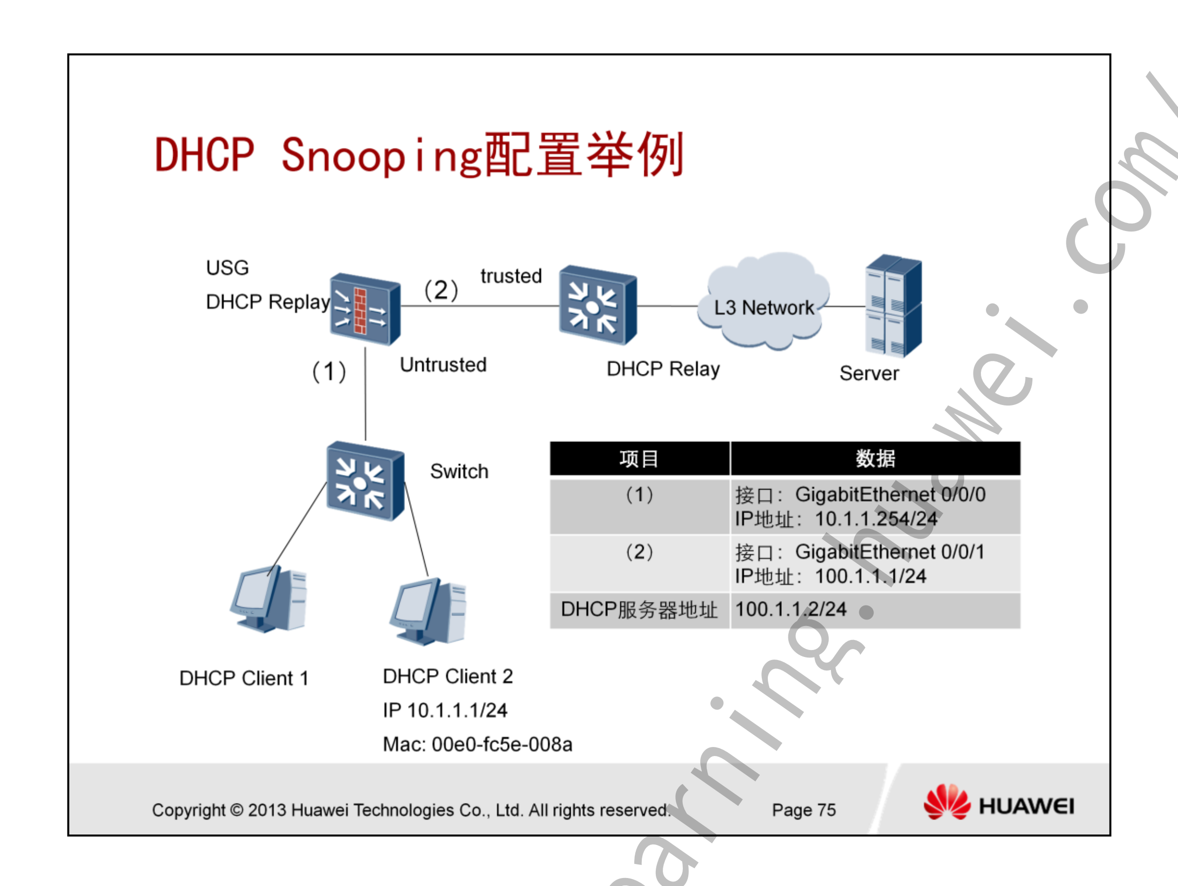
# DHCP Snooping典型应用场景

- DHCP Snooping功能用于防止:
  - DHCP Server仿冒者攻击;
  - 中间人攻击与IP/MAC Spoofing攻击;
  - 改变CHADDR值的DoS攻击;
  - Option82 。

| 攻击类型 | DHCP Snooping工作模式 |
|---|---|
| DHCP Server仿冒者攻击 | 信任（Trusted）/不信任（Untrusted） |
| 中间人攻击/IP/MAC Spoofing攻击 | DHCP Snooping绑定表 |
| 改变CHADDR值的DoS攻击 | 检查DHCP报文的CHADDR字段 |
| Option82 | MAC地址限制 |








| 项目 | 数据 |
|---|---|
| (1) | 接口：GigabitEthernet 0/0/0<br>IP地址：10.1.1.254/24 |
| (2) | 接口：GigabitEthernet 0/0/1<br>IP地址：100.1.1.1/24 |
| DHCP服务器地址 | 100.1.1.2/24 |

- 组网需求

如右图1所示，DHCP Client接入设备。要求在USG的三层接口GigabitEthernet 0/0/0和GigabitEthernet 0/0/1上配置DHCP Snooping功能。把DHCP Client侧的接口配置为untrusted模式，把DHCP Relay侧的接口配置为trusted模式。

- 要求USG可以防止以下类型的攻击：
  - DHCP Server仿冒者攻击；
  - 中间人攻击/IP/MAC Spoofing攻击；
  - 改变CHADDR值的DoS攻击；
  - 仿冒DHCP续租报文攻击；
  - 发送DHCP Request报文攻击,其中DHCP Clinet1使用动态分配的IP地址；DHCP Client2使用静态分配的IP地址。

# DHCP Snooping配置步骤（1）

**配置DHCP Relay的基本功能**

- 配置接口GigabitEthernet 0/0/1接口地址。

```
<USG> system-view
[USG] sysname DHCP-Relay
[DHCP-Relay] interface GigabitEthernet 0/0/1
[DHCP-Relay-GigabitEthernet0/0/1] ip address 100.1.1.1 24
```

- 配置DHCP中继功能接口。

```
[DHCP-Relay] interface GigabitEthernet 0/0/0
[DHCP-Relay-GigabitEthernet0/0/0] ip address 10.1.1.254 24
[DHCP-Relay-GigabitEthernet0/0/0] dhcp select relay
[DHCP-Relay-GigabitEthernet0/0/0] ip relay address 100.1.1.2
```






对于USG系列，将接口加入安全区域，并配置域间包过滤以保证网络基本通信正常。配置要实现DHCP中继功能的接口，为其配置IP地址和地址掩码，使其和DHCP Client属于同一个网段。

## DHCP Snooping配置步骤（2）

开启DHCP Snooping功能，配置Trusted接口

- 启用全局和接口的DHCP Snooping功能。

```
[DHCP-Relay] dhcp snooping enable
[DHCP-Relay] interface GigabitEthernet 0/0/0
[DHCP-Relay-GigabitEthernet0/0/0]dhcp snooping enable
[DHCP-Relay] interface GigabitEthernet 0/0/1
[DHCP-Relay-GigabitEthernet0/0/1]dhcp snooping enable
```

- 配置DHCP Server侧接口配置为“Trusted”。

```
[DHCP-Relay-GigabitEthernet0/0/1]dhcp snooping trusted
```







将连接DHCP Server侧的接口配置为“Trusted”，将连接DHCP Clinet侧的所有接口开启DHCP snooping（如果用户侧接口没有配置“Trusted”模式，那么开启了接口的Snooping特性后，接口模式默认为“Untrusted”），这样可以防止DHCP Server仿冒者攻击。

# DHCP Snooping配置步骤（3）

- 配置对特定报文的检查和DHCP Snooping绑定表

```
[DHCP-Relay] interface GigabitEthernet 0/0/0
[DHCP-Relay-GigabitEthernet0/0/0] dhcp snooping check arp enable
[DHCP-Relay-GigabitEthernet0/0/0] dhcp snooping check ip enable
[DHCP-Relay-GigabitEthernet0/0/0] dhcp snooping check dhcp-request enable
[DHCP-Relay-GigabitEthernet0/0/0] dhcp snooping check dhcp-chaddr enable
[DHCP-Relay-GigabitEthernet0/0/0] dhcp snooping bind-table static ip-address
10.1.1.1  mac-address 00e0-fc5e-008a
```





在DHCP Clinet侧的接口进行ARP报文和IP报文检查，这样可以防止中间人攻击/IP/MAC Spoofing攻击。在DHCP Clinet侧的接口进行DHCP Request报文检查，这样可以防止仿冒DHCP续租报文的攻击。在DHCP Clinet侧的接口进行CHADDR检查，这样可以防止改变CHADDR值的DoS攻击。配置静态绑定表项，对于使用静态分配IP的用户，需要单独配置DHCP Snooping静态绑定表项。

# DHCP Snooping配置步骤（4）

- 配置DHCP上送速率限制和配置Option82

```
[DHCP-Relay] dhcp snooping check dhcp-rate 90
[DHCP-Relay] dhcp snooping check dhcp-rate enable
[DHCP-Relay] interface GigabitEthernet 0/0/0
[DHCP-Relay-GigabitEthernet0/0/0] dhcp option82 insert enable
```

- 显示DHCP Snooping绑定表的静态表项信息。

```
<sysname> display dhcp snooping bind-table static
 bind-table:
ifname vrf     vsi     p/cvlan     mac-address      ip-address tp lease
Vlanif1 0000   -     0000/0000  0011-0022-0034    1.2.3.0    S   0
```







配置DHCP上送速率检查，这样可以防止DHCP Request报文攻击。配置DHCP报文中携带接口信息，以便建立精确的绑定表信息。

Ifname 配置绑定的接口名称
Vrf L3VPN标识，未绑定时为0
Vsi 虚拟交换实例的名称
p/cvlan Port VLAN和Client VLAN的值
mac-address 绑定的MAC地址
ip-address 绑定的IP地址



# 总结

- 网络攻击分类
- 各网络攻击分类的实现原理
- 不同类型的网络攻击的防范技术







# 思考题

- 防范流量型的攻击技术有哪些？防范原理是什么？
- 畸形报文攻击技术有哪些？防范原理是什么？
- 特殊报文攻击技术有哪些？防范原理是什么？
- 扫描窥探攻击技术有哪些？防范原理是什么？
- DHCP Snooping技术是什么？防范原理是什么？








- 判断题

  1. 畸形报文攻击与特殊报文攻击实现原理是一致的，只是名称不同而以。

- 单选题

  1. 以下哪个是流量型攻击?

  A. SYN Flood　B. ip-sweep　C. Port Scan　D. 以上都是








- 习题与答案：

  1、畸形报文攻击与特殊报文攻击实现原理是一致的，只是名称不同而以。

  答案：错误

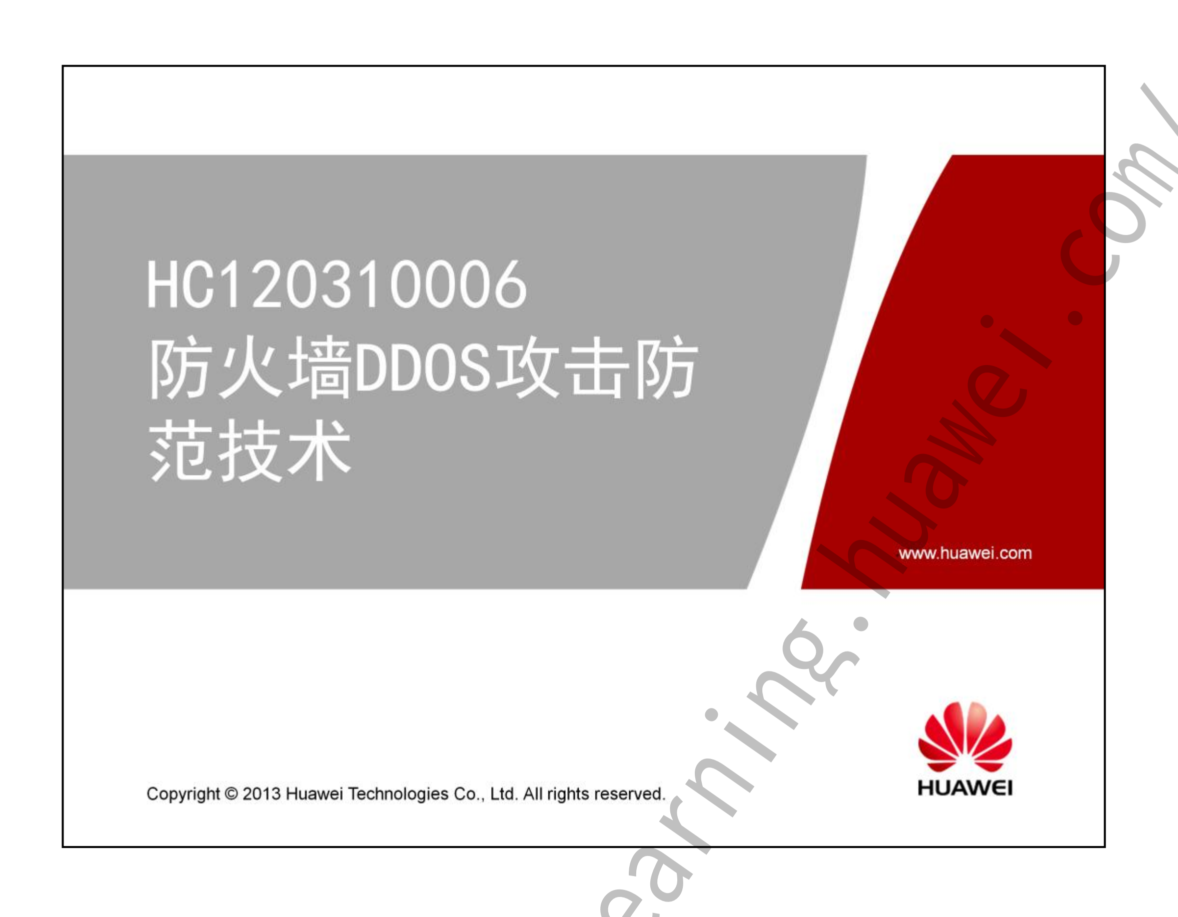
  2、以下哪个是流量型攻击?

  SYN Flood　B. ip-sweep　C. Port Scan　D. 以上都是

  答案：A

Thank you

www.huawei.com


HC120310006
防火墙DDOS攻击防范技术
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



# 目标

- 学完本课程后，您将能够:
  - 了解主要DDOS攻击的危害和原理
  - 了解DDOS攻击防范解决方案原理
  - 熟悉DDOS攻击防范解决方案组网规划
  - 掌握DDOS攻击防范解决方案安装配置步骤







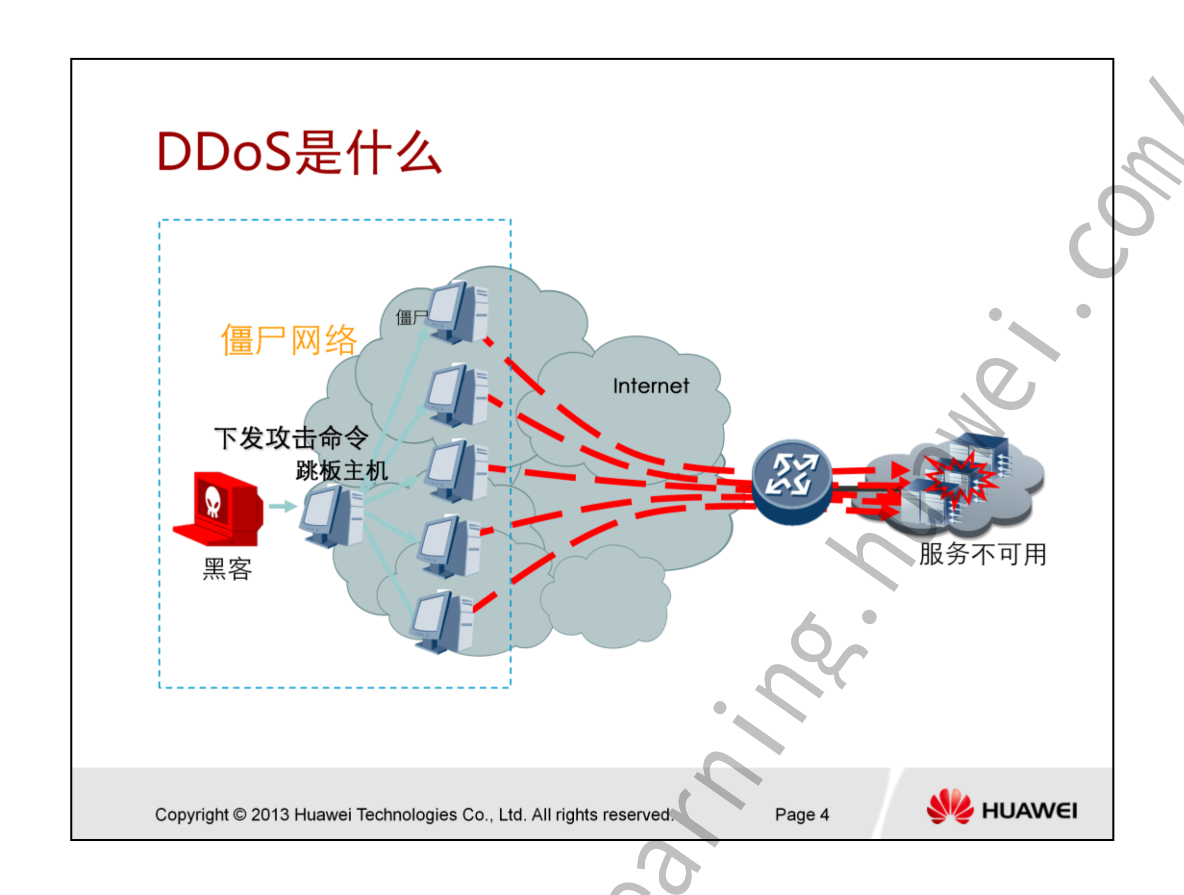

# 目录












- **何谓DoS攻击?**

最早的攻击形式是DoS（Denial of Service）攻击，即攻击者通过网络向攻击目标（一般是服务器，如DNS服务器、WEB服务器）发送少量非业务流量的异常报文，使被攻击服务器解析该类报文时系统崩溃或者系统繁忙，达到无法为正常用户提供服务的目的，即服务器拒绝为正常用户提供服务。

- **何谓DDoS攻击?**

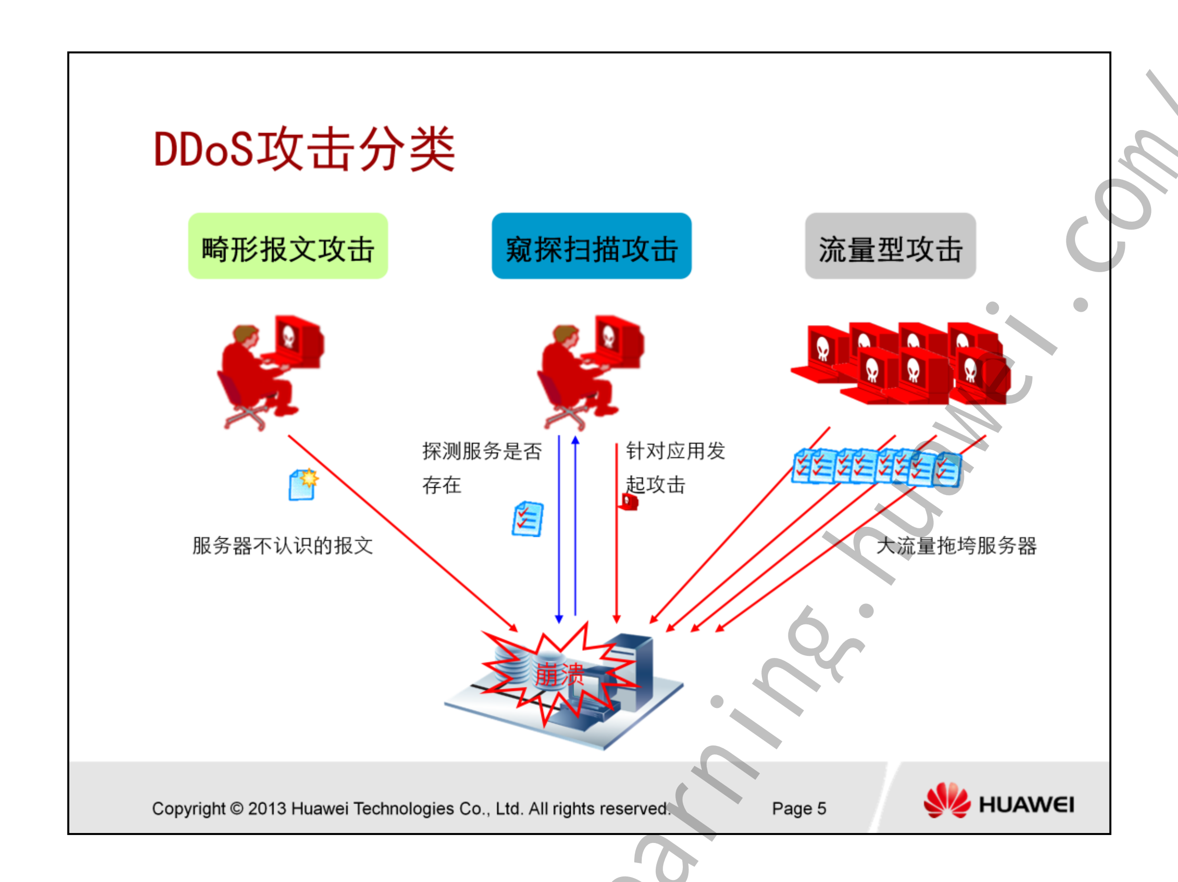
DDoS全称为Distributed Denial of Service，即分布式的DoS攻击。这类攻击通常都是通过僵尸网络发起的。因僵尸网络分布于互联网各处，因此这类攻击叫分布式DoS攻击。

- **用户的损失**

联众服务器在IDC最近一次的攻击受到的损失超过300万；完美时空服务器在IDC最近一次的攻击受到的损失超过350万。运营商据专业统计报告：IDC行业由于安全问题年损失3000万美元。

- **运营商的损失**

超大异常流量造成运营商网络带宽拥塞，导致运营商不断扩容链路和网络设备。某运营商网吧大客户由于连续遭到DDoS攻击，网速急剧变慢，连续数月，不断有用户退网。




- **畸形报文攻击**

利用操作系统或应用服务的漏洞，通过少量报文导致服务器操作系统或应用系统解析异常，甚至崩溃，如Winnuke、 Tear Drop。通过操作系统或应用加固即可有效防御该类攻击。

- **扫描窥探型攻击**

扫描类攻击：主机扫描和端口扫描，通过扫描获取网络可攻击的目标。

特殊控制报文：如TRACERT报文、IP路由记录选项控制报文，通过该类报文测探网络拓扑结构，做好攻击前准备工作。

上面两类攻击行为在攻击防范章节有详细介绍请参考，本节主要介绍流量型攻击行为。

- **流量型攻击**

当通过大量报文导致链路拥塞或者系统处理繁忙时，这类攻击我们叫流量型攻击，即flood攻击，Flood攻击以SYN Flood、UDP Flood、ICMP Flood为主要代表。

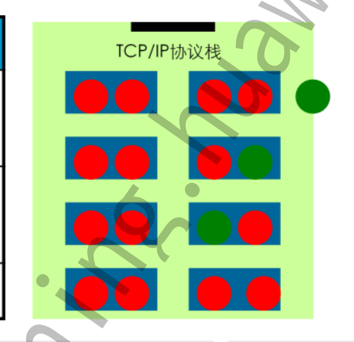
流量型攻击典型特点就是以众多的小流量汇聚成为大流量冲击服务器，以实现让服务器拒绝服务的目的，类似于“人海战术”。

近年又发展为针对常见服务的flood攻击，常见攻击有connection flood(连接耗尽)、HTTP Flood（攻击效果最明显的如CC攻击）、DNS Query Flood、DNS Reply Flood、SIP Flood（对SIP端口发送大量UDP垃圾报文）。

## 流量型攻击介绍—TCP类Flood攻击

TCP类型的Flood攻击，攻击者派遣大批虚假用户的TCP/IP协议栈里“占座”，导致正常用户没有“座位”；被攻击服务器接收到攻击报文后需要检查会话确认报文是否属于某个会话，如果攻击报文数量庞大，服务器处理性能耗尽。

| 攻击手段 | 服务器现象 |
| --- | --- |
| SYN Flood | 建立大量半连接，耗尽TCP资源 |
| SYN-ACK Flood | 协议栈忙于处理TCP连接，耗尽TCP资源 |
| ACK Flood | 带宽占满 |




 Page 6 HUAWEI

- **SYN-Flood攻击方式**

SYN Flood攻击往往伪造一个SYN报文，其源地址是伪造的，向服务器发起连接，服务器在收到报文后用SYN-ACK应答，而此应答发出去后，不会收到ACK报文，造成一个半连接。由于资源的限制，服务器的协议栈只能支持有限的TCP连接。如果攻击者通过僵尸网络发送大量这样的报文，会在被攻击主机上出现大量的半连接，消耗尽其资源，使正常的用户无法访问，直到半连接超时。因此，SYN Flood攻击也叫做半连接攻击。

- **ACK Flood攻击**

攻击者利用僵尸网络发起TCP后续包的Flood攻击，冲击网络带宽，造成网络链路拥塞。一般来说，携带负载的ACK报文会有效地挤占带宽。

- **SYN-ACK Flood攻击**

SYN-ACK Flood攻击源会假冒服务器，发送大量SYN-ACK报文到攻击目标网络或服务器，如果网络出口有状态防火墙，引起状态防火墙处理异常；如果报文目的端口是被攻击服务器的TCP服务端口，会引起服务器TCP协议栈处理异常。

# 流量型攻击介绍—UDP和ICMP Flood攻击

UDP和ICMP都是无连接的协议，因此此类Flood类攻击主要采用“人海战术”，堵住出口，无法进出的正常流量。如果针对服务器应用端口的Flood攻击，也会冲击服务器处理性能。

| 攻击手段 | 服务器现象 |
| --- | --- |
| UDP Flood | 带宽占满，网络拥塞 |
| UDP Fragment Flood | 带宽占满，网络拥塞；处理分片报文（分片缓存、重组）耗费资源 |
| ICMP Flood | 忙于回应，没空理会正常业务 |










- UDP Flood攻击

攻击者通过僵尸网络向目标服务器发起大量的UDP报文（一般为大包，应用程序存在时交到上层进行处理，若应用程序不存在则主机回应ICMP不可达报文）， 造成服务器资源耗尽，无法响应正常的请求，严重时会导致链路拥塞。

- UDP Fragment Flood攻击

攻击者向攻击目标发送大量的UDP分片报文，消耗带宽资源，造成被攻击者的响应缓慢甚至无法对外响应。当然分片还会引起协议栈更多的资源消耗，比如分片缓存和重组，所以更加消耗服务器处理性能。

- ICMP Flood攻击

发送大量的ICMP消息(如ping)到服务器，服务器会不断回应。严重时导致服务器无法处理合法的请求，甚至可能导致链路拥塞。

# 流量型攻击介绍—应用层Flood攻击

针对各种应用层协议Flood攻击，例如DNS Query Flood、HTTP GET Flood等。攻击原理各有区别，但攻击手段和网络层攻击类似。

| 攻击手段 | 目标应用 | 攻击原理 |
|---|---|---|
| DNS Query Flood | DNS 服务器 | 伪造大量DNS请求，造成DNS服务器瘫痪。 |
| DNS Reply Flood | DNS 服务器或某台主机 | 伪造大量DNS回应报文，将一些合法域名指向恶意IP地址 |
| HTTP GET/POST Flood | WEB服务器 | 大量HTTP Get/Post报文，请求涉及数据库操作的URL或其它消耗系统资源的URL |
| HTTPS Flood | 一般针对网银 | 大流量HTTPS连接请求，消耗资源 |
| SIP Flood | SIP服务器 | 发送大量INVITE消息到SIP服务器，导致SIP服务器拒绝服务 |
| Connection Flood | 具体应用服务器 | 建立大量TCP连接，耗尽服务器资源 |

 Page 8 

- DNS Query Flood攻击

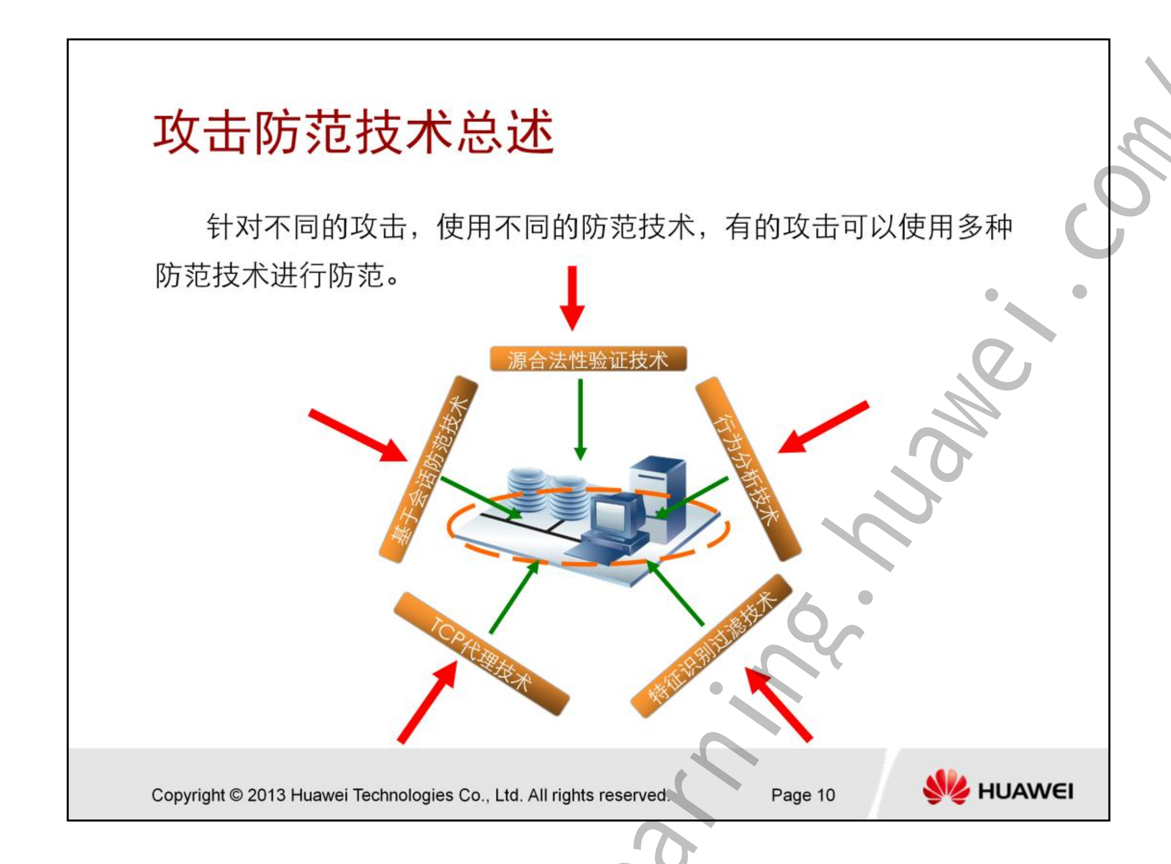
攻击者通过僵尸网络向DNS服务器发送大量不存在的域名解析请求，致使DNS服务器严重超载，无法继续响应正常用户的DNS请求，从而达到攻击的目的。该类攻击的源IP一般都是虚假的，而且为了达到大面积攻击效果，攻击者一般将报文的递归查询字段置位，当前服务器查询不到会向其上级服务器请求，导致众多DNS服务器发生连锁反应。访问互联网资源，必须通过DNS域名请求，因此该类攻击的危害性极大，往往因DNS服务器的决绝服务导致大面积的网络访问变慢，甚至瘫痪。

- DNS reply Flood攻击

DNS Reply Flood也可称为DNS Spoofing，是指攻击者在一定条件下将大量伪造的DNS应答包发送给某个DNS Server或某台主机，这些应答包将一些合法域名指向恶意IP地址，从而达到欺骗接收者、干扰网络的目的。

- HTTP Get/Post Flood攻击

也叫CC攻击，攻击者通过代理或者通过僵尸向目标服务器发起大量的HTTP Get/Post报文，请求涉及数据库操作的URL或其它消耗系统资源的URL，造成服务器资源耗尽，无法响应正常请求。 利用僵尸网络发起的针对Web 服务器消耗CPU资源的URL的攻击，如需要访问数据库的URL，攻击速率可能并不快，但攻击源分布很广，攻击效果明显。




华为异常流量清洗解决方案中，对各种攻击有多种防范方式，归纳起来主要有5种。

- TCP代理技术

  防火墙接管对服务器的TCP连接，以进行检测和防范。

- 源合法性验证技术

  通过基于传输协议的源认证技术和基于应用协议的源认证技术，鉴别报文源是合法用户还是攻击者，以达到防范的目的。

- 行为分析技术

  攻击往往都有一些行为特征，比如资源访问固定，访问频率恒定等，通过此检测技术检查出攻击报文。

- 基于会话防御技术

  通过会话状态来识别攻击报文。

- 特征识别过滤技术

  在以上检测都无效或者无法防御的情况下，可以使用特征识别过滤技术，找出攻击报文的负载特征，作为流量过滤条件，手动进行特征编辑，防范某些攻击。



# 目录







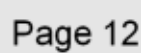



# 目录

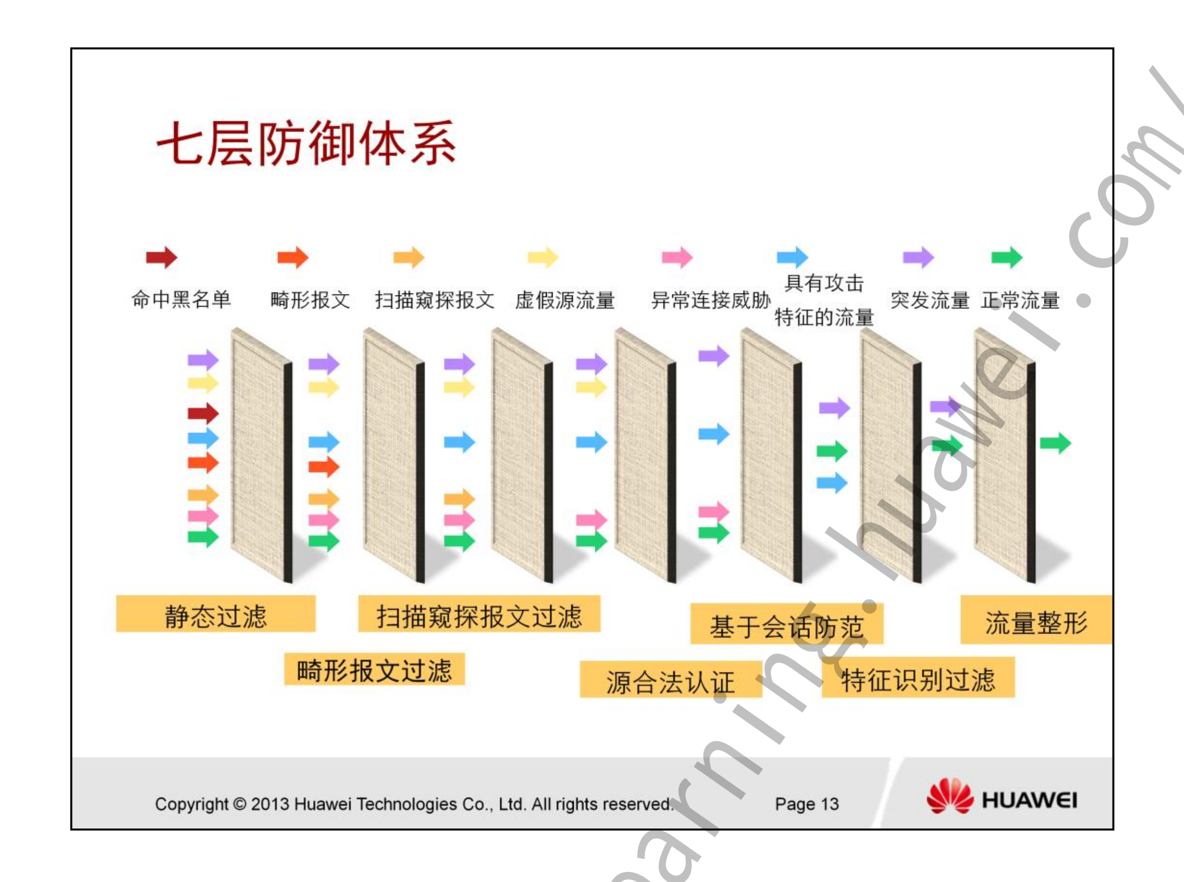













静态过滤：直接丢弃位于黑名单中的IP地址发出的流量，或者直接让位于白名单的IP地址发出的流量通过。

畸形报文过滤：过滤利用协议栈漏洞的畸形报文攻击。

扫描窥探报文过滤：过滤探测网络结构的扫描型报文和特殊控制报文。

源合法性认证：基于应用来认证报文源地址的合法性，这些应用支持协议交互。清洗设备通过发送源探测报文及检查响应报文来防范虚假源或工具发出的攻击流量。

基于会话防范：基于会话来防御并发连接、新建连接或异常连接超过阈值的连接耗尽类攻击。

特征识别过滤：主要靠指纹学习和抓包分析来获得流量特征，防范僵尸工具或通过代理发起的攻击流量，以区别正常用户的访问行为。

其中抓包分析是指对异常/攻击流量抓包以生成抓包文件，通过对抓包文件进行解析和提取指纹，能够获取流量特征。

流量整形：流量经过此前各分层过滤之后，流量依然很大，超过用户实际带宽，此时采用流量整形技术，确保用户网络带宽可用。

## 具体防御策略

- 七层防御技术是通过在Anti-DDoS设备上配置防御策略来实现的。
  - 基于接口
  - 基于全局
  - 基于防护对象








**基于接口的防御**

在配置防御策略时，管理员应该首先配置基于接口的防御策略，以应对大流量攻击。Anti-DDoS设备在收到报文时，首先在接口板对报文进行合法性检查。通过认证的报文允许通过；没有认证通过的报文禁止通过。

**基于全局的防御**

配置全局防御方式后，设备对流经的所有流量进行检测和清洗，不区分流量属于哪个防护对象。

**基于防护对象的防御**

基于网段的防御。基于网段的防御是指针对整个防护对象设置防御阈值，将每个防护对象的所有目的IP流量集中统计，一旦流量达到告警阈值则触发防御。

基于服务的防御。清洗设备将到达防护对象的流量按照目的IP地址、协议类型和目的端口，定义为不同的服务类型，针对不同类型的服务配置不同的防御策略，进行精细化防御和差异化防御。

基于防护对象的默认防御策略。默认防御策略中的各种防御方式主要是针对非服务流量进行防御的。到达防护对象的流量中，通常除了服务流量外，还有很多非服务流量。这些非服务的流量有的是用户操作产生的流量（比如：Telnet、Ping等），有的是冗余或者攻击流量，针对不同类型的流量，可以配置不同的防御手段。

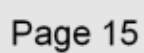


# 目录





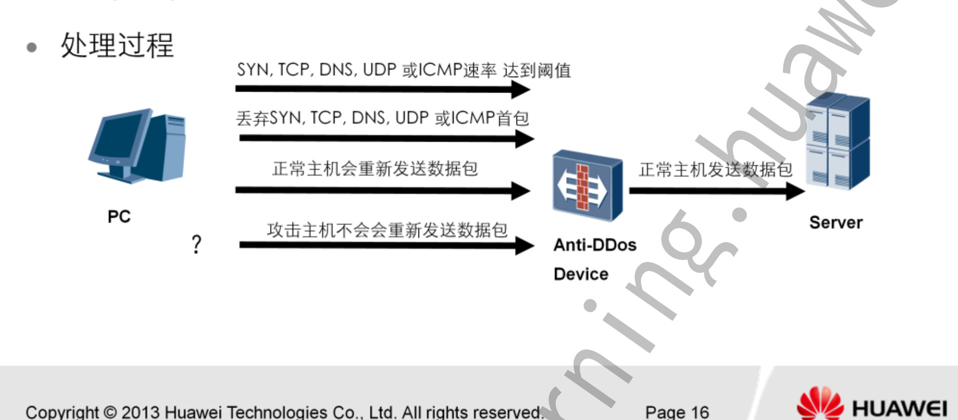






## 首包丢弃

- 首包丢弃
  - 有些攻击是不断变换源IP地址或者源端口号发送攻击报文，通过首包丢弃，可以有效拦截这部分流量。首包丢弃与源认证结合使用，防止虚假源攻击。
- 处理过程








- 处理过程

开启首包丢弃功能后，SYN、TCP、DNS、UDP、ICMP各类流量超过阈值后，设备会丢弃报文首包。

基于三元组（源IP地址、源端口和协议）来匹配报文，并通过报文的时间间隔来判断首包：

当报文没有匹配到任何三元组时，认为该报文是首包，将其丢弃。

当报文匹配到某三元组，则计算该报文与匹配该三元组的上一个报文到达的时间间隔。

如果时间间隔低于设定的下限，或者高于设定的上限，则认为是首包，将其丢弃；如果时间间隔落在配置的上限和下限之间，则认为是后续包，将其放行



# 目录









# 阻断和限流

- 通过服务学习或经验发现网络中根本没有某种服务或某种服务流量很小，则可以分别采用阻断和限流方法来防御攻击。
  - 阻断：在自定义服务策略中表示将匹配自定义服务的报文全部丢弃；在默认防御策略中表示将自定义服务以外的此协议报文全部丢弃。
  - 限流：在自定义服务策略中表示将匹配自定义服务的报文限制在阈值内，丢弃超过阈值的部分报文；在默认防御策略中表示将自定义服务以外的此协议报文限制在阈值内，丢弃超过阈值的部分报文







# 目录









## 静态指纹过滤

- 通过配置静态指纹，对命中指纹的报文进行相应的处理，从而对攻击流量进行防御。
  - TCP/UDP/自定义服务可基于载荷（即报文的数据段）提取指纹
  - DNS报文针对域名提取指纹
  - HTTP报文针对通用资源标识符URI（Uniform Resource Identifier）提取指纹。







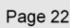
可与抓包取证结合，提取流量特征，作为过滤条件。支持基于异常事件自动抓包，抓包支持抽样比，可对攻击流量进行均匀、全面抓包，忽略正常流量特征，准确提取异常流量特征。



# 目录

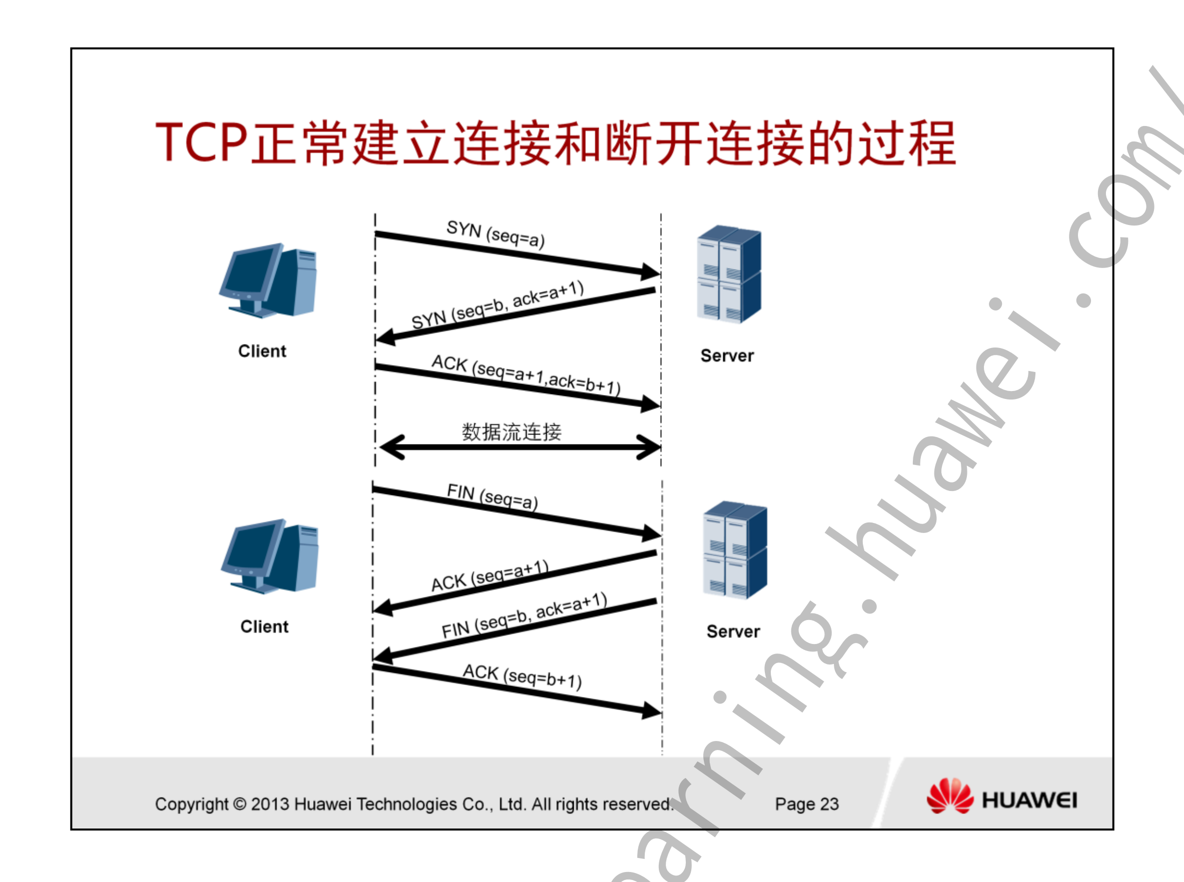













- 在TCP/IP协议中，TCP协议提供可靠的连接服务，采用三次握手建立一个连接。

第一次握手：建立连接时，客户端发送SYN包(SYN=J)到服务器，并进入SYN_SENT状态，等待服务器确认。

第二次握手：服务器收到SYN包，必须发出ACK包（ACK=J+1）来确认客户端的SYN包，同时自己也发送一个SYN包（SYN=K），即SYN-ACK包，此时服务器进入SYN_RCVD状态。

第三次握手：客户端收到服务器的SYN-ACK包，向服务器发送确认包ACK(ACK=K+1)，此包发送完毕，客户端和服务器进入ESTABLISHED状态，完成三次握手。

如果服务器发出的SYN-ACK包异常，客户端会发送一个RST包给服务器，服务器重新回到LISTEN监听状态。

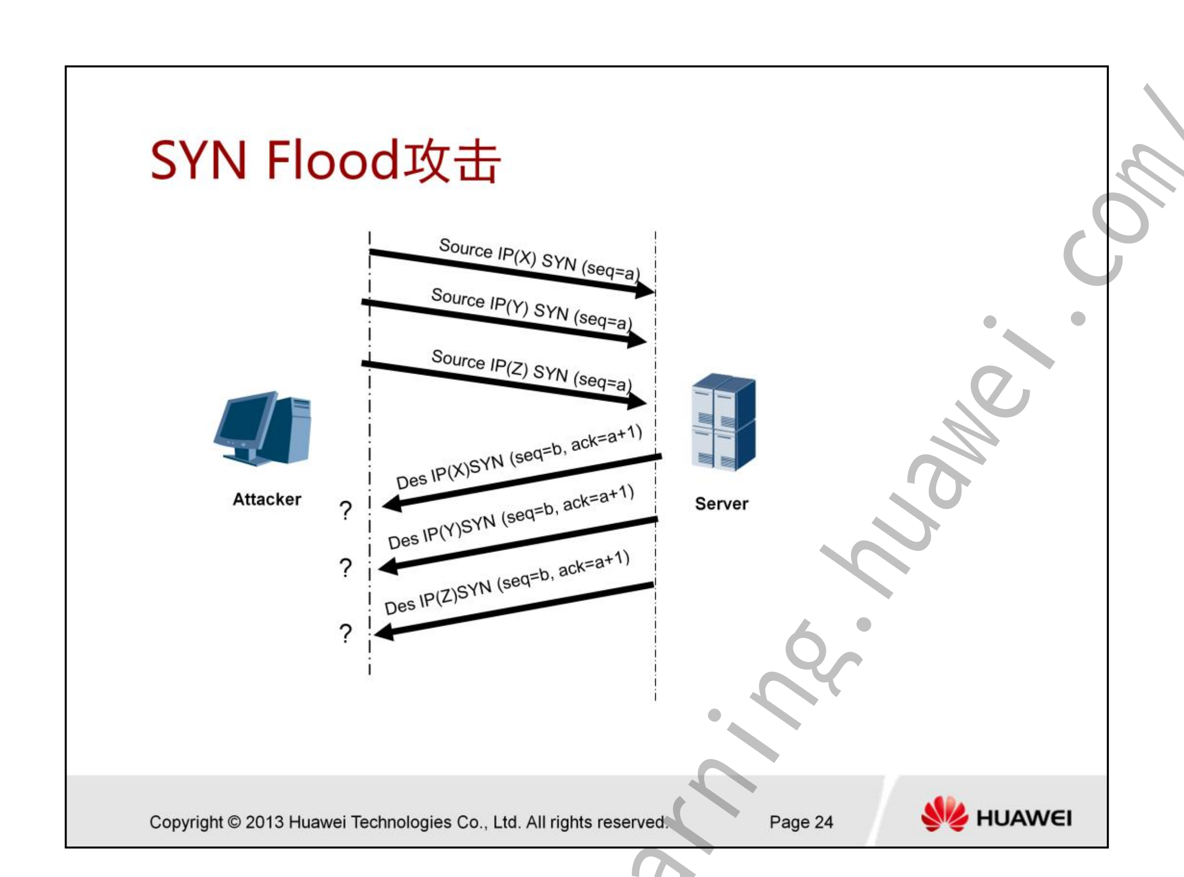
- TCP采用四次握手来关闭一个连接。

第一次握手：客户端发送FIN包（FIN=M）到服务器，表示客户端没有数据要向服务器发送了，同时进入FIN_WAIT_1状态，等待服务器确认。

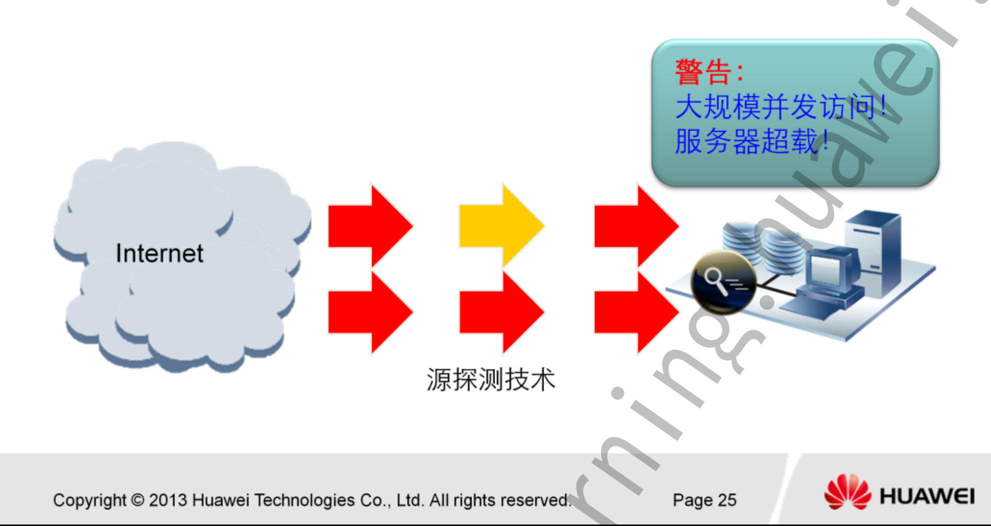
第二次握手：服务器收到FIN包，必须发送ACK包（ACK=M+1）来确认客户端的FIN包，但服务器数据还没传完，所以不发送FIN包，此时服务器进入LAST_WAIT状态。

第三次握手：当服务器没有数据要向客户端发送时，服务器发送FIN包（FIN=N）到客户端，并进入LAST_ACK状态，等待客户端最终确认。

第四次握手：客户端收到FIN包，发出ACK包（ACK=N+1）来确认服务器的FIN包，进入TIME_WAIT状态，等待连接完全断掉。此包发送完毕，服务器进入CLOSED状态，完成四次握手，双方连接断开。


SYN Flood攻击
Source IP(X) SYN (seq=a)
Source IP(Y) SYN (seq=a)
Source IP(Z) SYN (seq=a)
Attacker
Server
Des IP(X)SYN (seq=b, ack=a+1)
Des IP(Y)SYN (seq=b, ack=a+1)
Des IP(Z)SYN (seq=b, ack=a+1)
?
?
?
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 24
HUAWEI



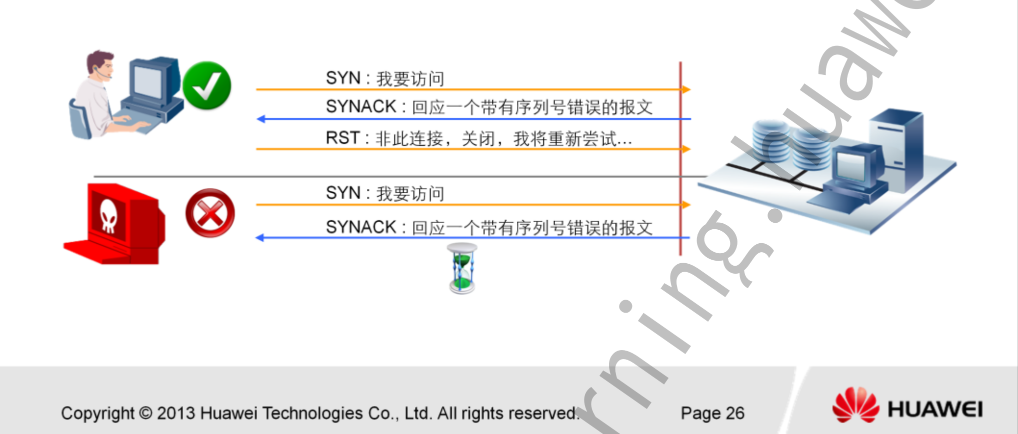



基于传输协议层的源验证技术主要是防范虚假源攻击，基于应用协议的源验证技术主要是防非应用客户端攻击。



# 基于传输协议层的源合法性验证技术

利用TCP协议原理，针对TCP类Flood进行检测和防御。用户进行TCP连接，清洗设备回应经过构造的SYN-ACK报文，通过用户的反应来判断此用户是否正常。主要用于来回路径不一致的情况下。



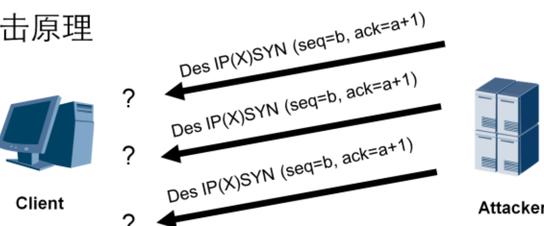



HUAWEI

来回路径不一致只可以用源合法性验证技术，但来回路径一致情况下也可以使用反向探测技术。反向探测技术性能很高，大流量冲击情况下防范效果更好。

# SYN-ACK Flood攻击与防御原理

- 通过对报文源的合法性检查来防御SYN-ACK Flood攻击。
- 攻击原理




- 防御原理
  - 清洗设备基于目的地址对SYN-ACK报文速率进行统计，当SYN-ACK报文速率超过阈值时，启动源认证防御。






**攻击原理**

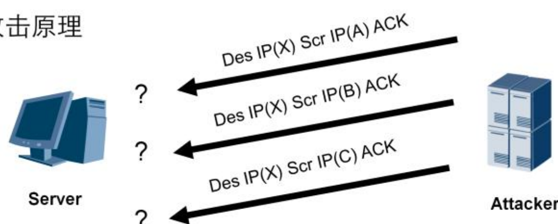
SYN-ACK Flood攻击源会假冒服务器，发送大量SYN-ACK报文到攻击目标网络或服务器，如果网络出口有状态防火墙，引起状态防火墙处理异常；如果报文目的端口是被攻击服务器的TCP服务端口，会引起服务器TCP协议栈处理异常。

**防御原理**

清洗设备基于目的地址对SYN-ACK报文速率进行统计，当SYN-ACK报文速率超过阈值时，启动源认证防御。

# ACK Flood攻击与防御原理

- 会话检查和载荷检查结合来防御ACK Flood攻击。
- 攻击原理




- 防御原理
  - 当ACK报文速率超过阈值时，启动会话检查。
    - 如果清洗设备检查到ACK报文没有命中会话，通过严格模式或者基本模式处理。
    - 如果清洗设备检查到ACK报文命中会话，则检查会话创建原因。
  - 载荷检查是清洗设备对ACK报文的载荷进行检查，如果载荷内容全一致（如载荷内容全为1等），则丢弃该报文。






**攻击原理**

攻击者利用僵尸网络发送大量的ACK报文，冲击网络带宽，造成网络链路拥塞；同时被攻击服务器接收到攻击报文后需要检查会话以确认报文是否属于某个会话，如果攻击报文数量庞大，服务器处理性能耗尽，从而拒绝正常服务。

**防御原理**

当ACK报文速率超过阈值时，启动会话检查。

如果清洗设备检查到ACK报文没有命中会话，则有两种处理模式：

“严格模式”：直路部署组网中建议采用“严格模式”。如果清洗设备没有检查到已经建立的会话，直接丢弃报文。

“基本模式”：旁路部署动态引流时，对于引流前已经建立的会话，清洗设备上会检查不到会话，此时建议采用“基本模式”，即当连续一段时间内ACK报文速率超过阈值时，启动会话检查，设备会先让几个ACK报文通过，建立会话，然后对会话进行检查，确定是否丢弃报文。

如果清洗设备检查到ACK报文命中会话，则检查会话创建原因。

如果会话是由SYN或SYN-ACK报文创建的，则允许该报文通过。

如果会话是由其他报文创建的（例如ACK报文），则查看报文检查结果，序列号正确的报文允许通过，不正确的报文则被丢弃。

载荷检查是清洗设备对ACK报文的载荷进行检查，如果载荷内容全一致（如载荷内容全为1等），则丢弃该报文。

只有启用了“会话检查”，才能启用“载荷检查”，对会话检查通过的报文进行载荷检查。

# FIN/RST Flood攻击与防御原理

- 防御FIN/RST Flood攻击的方法是进行会话检查
- 攻击原理



- 防御原理
  - 当FIN/RST报文速率超过阈值时，启动会话检查。
    - 如果清洗设备检查到FIN/RST报文没有命中会话，直接丢弃报文。
    - 如果清洗设备检查到FIN/RST报文命中会话，则检查会话创建原因。





**防御原理**

当FIN/RST报文速率超过阈值时，启动会话检查。

如果清洗设备检查到FIN/RST报文没有命中会话，直接丢弃报文。

如果清洗设备检查到FIN/RST报文命中会话，则检查会话创建原因。

如果会话是由SYN或SYN-ACK报文创建的，则允许该报文通过。

如果会话是由其他报文创建的（例如ACK报文），则查看报文检查结果，序列号正确的报文允许通过，不正确的报文则被丢弃。

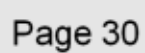


# 目录





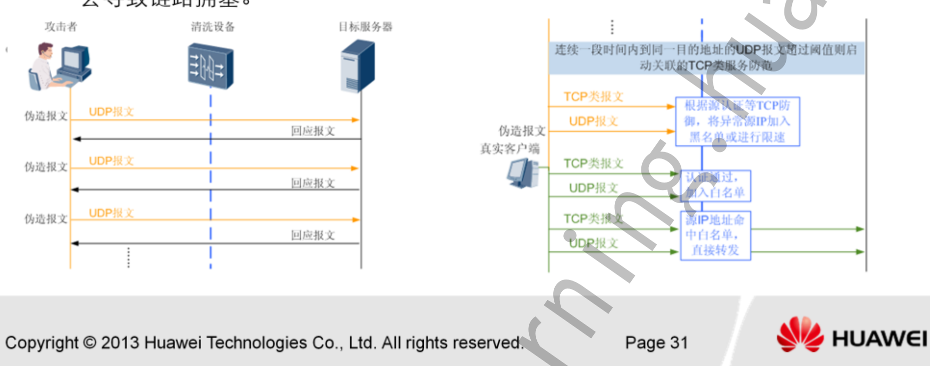






## UDP Flood关联TCP类服务防范

- 当UDP流量与TCP类服务有关联时，通过防御TCP类服务来防御UDP Flood
- 攻击原理
  - 攻击者通过僵尸网络向目标服务器发起大量的UDP报文，这种UDP报文通常为大包，且速率非常快，从而造成服务器资源耗尽，无法响应正常的请求，严重时会导致链路拥塞。






HUAWEI

UDP是无连接的协议，因此无法通过源认证的方法防御UDP Flood攻击。但是有些服务例如游戏类服务，是先通过TCP协议对用户进行认证，认证通过后使用UDP协议传输业务数据，此时可以通过防御UDP Flood关联的TCP类服务来达到防御UDP Flood攻击的目的，当发现源IP异常时，将TCP服务和UDP服务流量都丢弃或限速。

# 载荷检查和指纹学习

- 使用载荷检查和指纹学习方法防御具有规律的UDP Flood攻击。
- 攻击原理
  - 攻击者通过僵尸网络向目标服务器发起大量的UDP报文，这种UDP报文通常为大包，且速率非常快，从而造成服务器资源耗尽，无法响应正常的请求，严重时会导致链路拥塞。
- 防御原理

攻击者
清洗设备
目标服务器
伪造报文
UDP报文
回应报文
连续一段时间内到同一目的地址的UDP报文或分片报文超过阈值则启动指纹学习
指纹学习
真实客户端
转发未匹配指纹的UDP报文





HUAWEI

载荷检查：当UDP流量超过阈值时，会触发载荷检查。如果UDP报文数据段内容完全一样，例如数据段内容都为1，则会被认为是攻击而丢弃报文。

指纹学习：当UDP流量超过阈值时，会触发指纹学习。指纹由清洗设备动态学习生成，将攻击报文的一段显著特征学习为指纹后，匹配指纹的报文会被丢弃。

# UDP分片攻击与防御原理

- 使用载荷检查和指纹学习方法防御具有规律的UDP分片报文攻击。
- 攻击原理
  - 攻击者向攻击目标发送大量的UDP分片报文，消耗带宽资源，造成被攻击者的响应缓慢甚至无法正常回应。
- 防御原理
  - 载荷检查
  - 指纹学习







# 目录









# HTTP Flood攻击与防御原理

- 防御HTTP Flood攻击的方法包括源认证、目的IP的URI检测和指纹学习
- 攻击原理
  - 攻击者通过代理或僵尸向目标服务器发起大量的HTTP报文，请求涉及数据库操作的URI或其它消耗系统资源的URI，造成服务器资源耗尽，无法响应正常请求。
- 防御原理
  - **HTTP Flood源认证**
  - **目的IP的URI检测**
  - 指纹学习







# HTTPS类报文攻击防御

- 通过源认证方法来防御HTTPS Flood攻击。
- 攻击原理
  - 攻击者通过代理、僵尸网络或者直接向目标服务器发起大量的HTTPS连接，造成服务器资源耗尽，无法响应正常的请求。
- 防御原理
  - 通过源认证对HTTPS攻击进行防御，清洗设备基于目的地址对HTTPS请求报文速率进行统计，当HTTPS请求速率超过阈值时，启动源认证防御。





# SSL DoS攻击与防御原理

- 通过源认证和SSL防御结合防御SSL DoS攻击。
- 攻击原理
  - SSL握手的过程中，在协商加密算法时服务器CPU的开销是客户端开销的15倍左右。攻击者利用这一特点，在一个TCP连接中不停地快速重新协商。
- 防御原理
  - 清洗设备基于目的地址对HTTPS请求报文速率进行统计，当HTTPS请求速率超过阈值时，启动源认证防御和SSL防御：
    - 源认证
    - SSL防御







源认证：可参考HTTPS Flood攻击与防御原理

SSL防御：在检查周期内，如果某个源IP地址到目的IP地址的协商次数超过最大值，则将此会话标记为异常会话，在异常会话检查周期内，如果异常会话数超过最大值时，判定该源IP地址异常，将该源IP地址加入黑名单。



# 目录

1. 常见DDoS攻击技术介绍
2. **DDOS攻击防范技术**
   - 2.1七层防御体系
   - 2.2 首包丢弃
   - 2.3 阻断和限流
   - 2.4 静态指纹过滤
   - 2.5 TCP报文攻击防御
   - 2.6 UDP报文攻击防御
   - 2.7 HTTP或者HTTPS报文攻击防御
   - **2.8 其他报文攻击防御**
3. DDOS攻击防范组网配置






# DNS交互过程

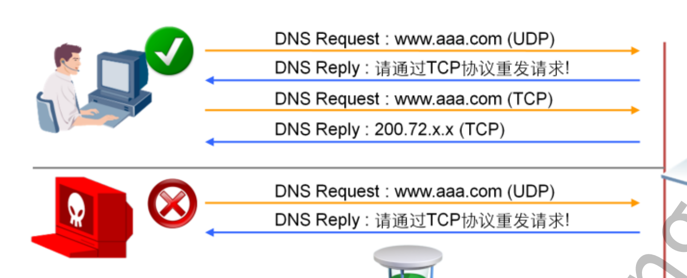
- 当用户上网访问某个网站时，会向DNS缓存服务器发出该网站的域名，以请求其IP地址。 DNS缓存服务器会直接用缓存区中的记录信息回应，直到该记录老化，被删除。
- 当DNS缓存服务器查找不到该域名与IP地址对应关系时，它会向授权DNS服务器发出域名查询请求。






# DNS Request Flood攻击与防御原理

利用应用层协议原理的具体原理，针对不同的应用协议进行检测防范。当用户发起请求，清洗设备回应经过构造的应用层报文，通过用户的反应来判断此用户是否正常。









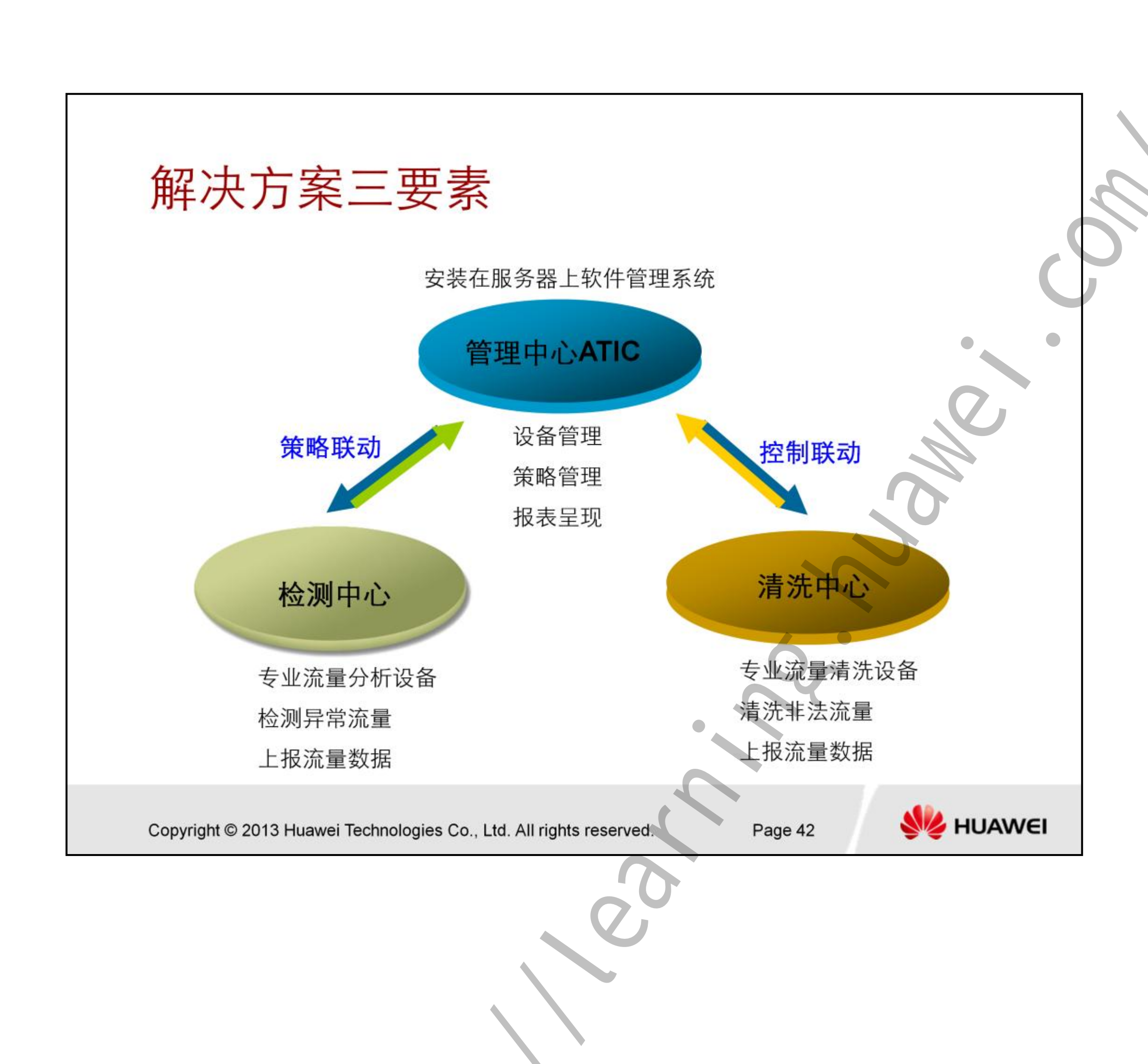

# 目录

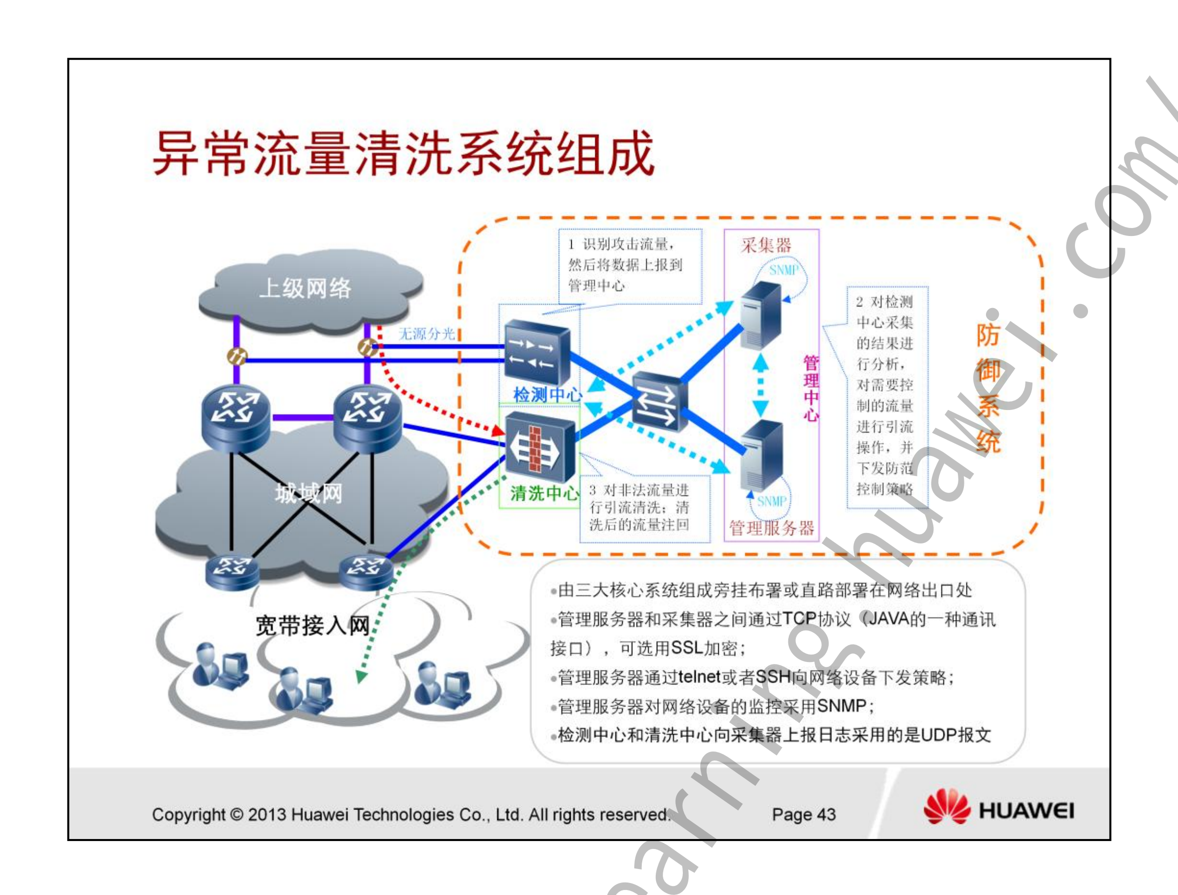









解决方案三要素
安装在服务器上软件管理系统
管理中心ATIC
设备管理
策略管理
报表呈现
策略联动
控制联动
检测中心
专业流量分析设备
检测异常流量
上报流量数据
清洗中心
专业流量清洗设备
清洗非法流量
上报流量数据
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 42
HUAWEI




该异常流量清洗方案系统主要包括三个组成部分：

- 检测中心

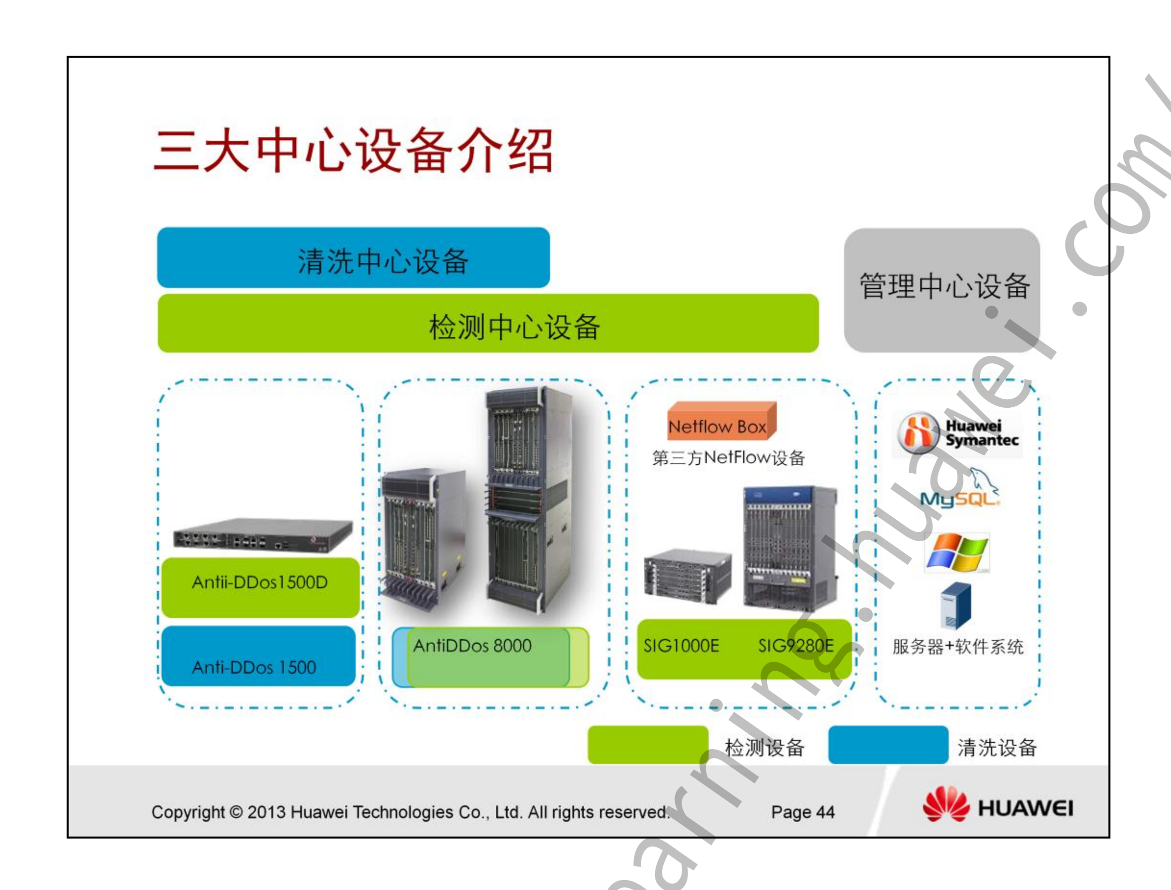
对镜像或者分光过来的流量进行DDoS攻击流量的检测和分析，将分析数据提供给管理中心进行判断。

- 管理中心

由服务器系统组成，也称之为ATIC管理系统。完成攻击事件的处理、并控制清洗中心的引流策略和清洗策略。并且对各种攻击事件和攻击流量的分类查看，并可产生报表。

- 清洗中心

由执行清洗任务的硬件系统组成，主要是根据安全管理中心的控制策略进行攻击流量牵引并清洗，把清洗后的正常流量注回到客户网络，发送到真正的目的地。




- 检测设备可由下列设备组成

  USG5300ADI；

  USG9300检测板；

  SIG系列产品；

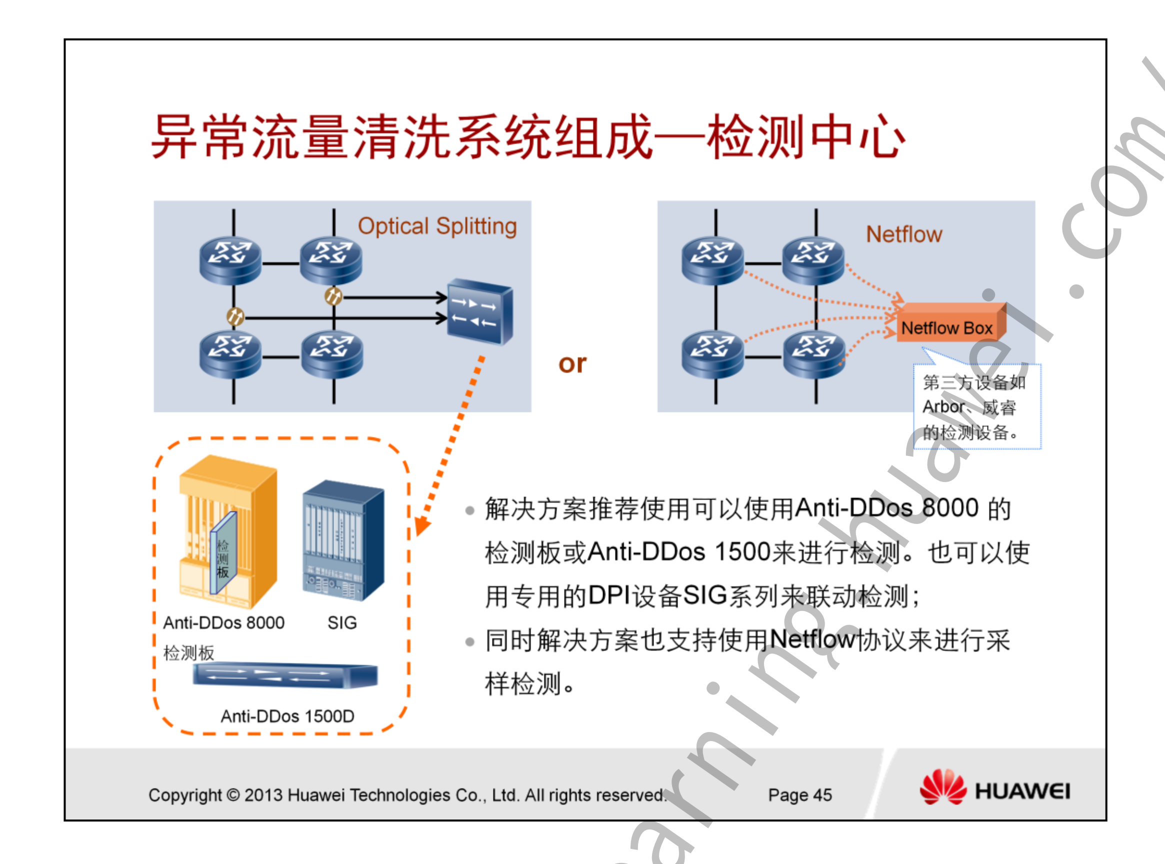
  第三方NetFlow设备。

- 清洗设备可由下列设备组成

  USG5300ADD；

  USG9300清洗板。

- 后台服务器需安装windows 2003 SP2操作系统




检测、监控中心主要负责网络流量的检测分析。

采用镜像或分光的方式，只需在将原来的光链路替换为分光器即可，常用的分光器有1分2、1分3等，光功率比有50：50、70：15：15等。或者在出口设备上将上下行的流量通过端口镜像方式引入到检测中心设备。

**主要特点**：

检测中心检测的是全部流量，因此检测准确率较高；

数据时间粒度可以很细，实时性较好；

包含7层协议信息，并可实现其他应用层异常分析检测；

检测准确度高，深度包检测，特征匹配，会话重组；

部署集中，扩展性要求较高，旁路部署对现网设备无任何影响。

如果使用Netflow协议，那么要求网络设备支持Netflow协议，对网络流量进行采样分析。这样的话，并不能分析所有流量，因此检测准确率较低，其主要特点如下：

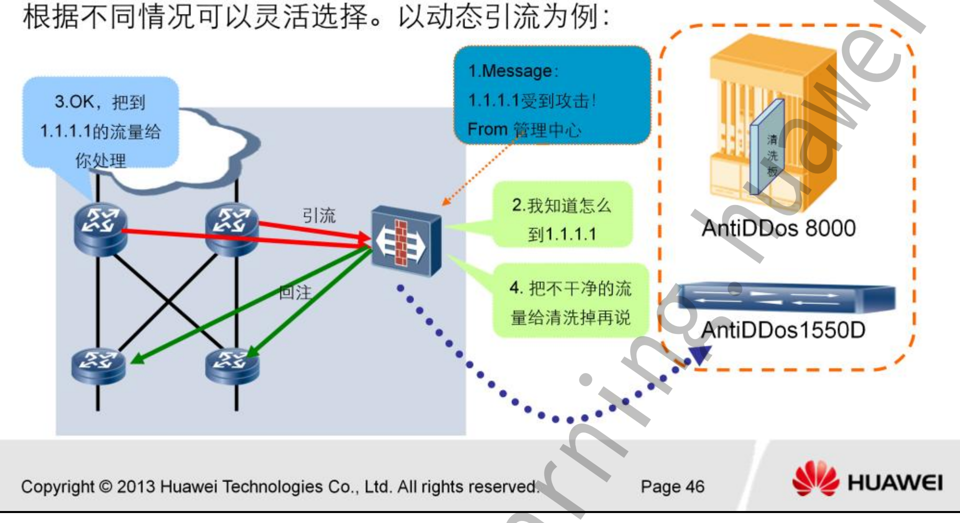
数据时间粒度中等，有些延迟；

无法做到精细化的检测，而精细化的检测对行业网来说非常重要；

抽样比较大，不适合做小流量攻击检测，不包含应用层信息；

部署简单，易于扩展；

需要现网设备向分析设备发送Netflow流，对现网设备有一部分的影响。




- 引流方式有两种：

**静态引流**：核心设备上通过路由方式或者策略路由方式将流量引到清洗设备上；

**动态引流**：通过BGP实现动态引流。清洗中心通过与核心设备建立BGP邻居。通告一到目的地址的主机路由，将流量“骗”过来，清洗后再回注回去。这条主机路由是管理中心动态下发的一条静态路由，并且已经引入了BGP。

- 回注方式有如下几种：

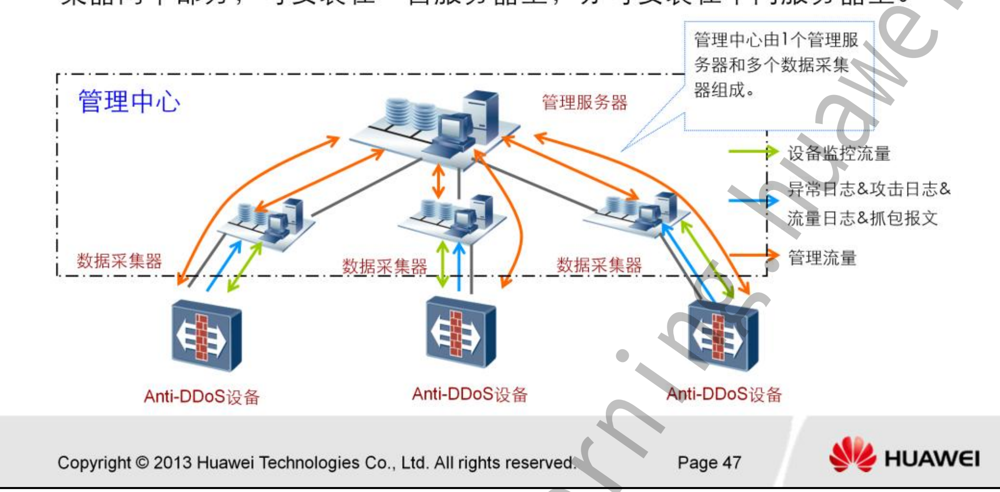
**策略路由回注**：通过策略路由将清洗后流量回注；

**路由回注**：通过默认路由或者其他动态路由方式回注；

**VPN回注**：通过GRE VPN或者MPLS VPN方式回注；

**二层回注**：如果上下行在一个网段，通过二层回注。

清洗设备支持丰富灵活的攻击防范技术，可有效防范SYN Flood、UDP Flood、CC攻击、ICMP Flood等各种攻击手段。可以防范十多种DDoS攻击，主要包括：SYN Flood攻击、ICMP Flood、UDP Flood攻击、Land攻击、Smurf攻击、Fraggle攻击、WinNuke攻击、ICMP重定向或不可达报文等。同时将这些攻击行为记录在日志中。




异常流量清洗解决方案采用B/S架构，部署简单方便，不需安装客户端软件即可完成业务的管理和监控，适合客户多地域分散部署多台检测和清洗设备，而通过一台设备集中管理。作为方案管理平台，系统支持SIG检测设备、USG5300ADD和USG9300清洗设备的联动配置和管理。系统支持分权分地域管理，不仅能作为单台清洗设备的管理平台，亦可作为多台清洗设备和检测设备的集中管理平台。

管理中心设备分为两个组件：

**数据采集器：**一台清洗设备对应一台数据采集器，数据采集器负责异常流量清洗业务数据采集、解析、汇总、入库并负责将汇总后的流量上报管理服务器用以报表呈现；

**管理服务器：**负责异常流量清洗方案设备集中管理配置及业务报表呈现。

支持分布式部署集中管理：数据采集器和管理服务器支持分布式部署和集中式部署两种部署模式；分布式部署模式下具备很好的可扩展性，管理服务器可同时管理50台DDoS防御设备。

整个系统基于大客户管理，充分体现了以客户为中心的管理理念，基本策略都以策略模板的形式呈现，可以自由绑定给不同的大客户。

报表呈现形式直观、多样，可提供基于大客户的报表亦可提供运营商报表。可根据用户需求灵活定制报表内容，支持报表自动导出。报表呈现粒度多样，能满足各种运营需求。



# 目录









# 直路部署方式

客户网络 | 直路部署（主备方式）

Internet

清洗中心

FW

SW

Web

Mail

DMZ

OA

Trust

管理中心

清洗前流量

日志流量

清洗后流量

管理流量

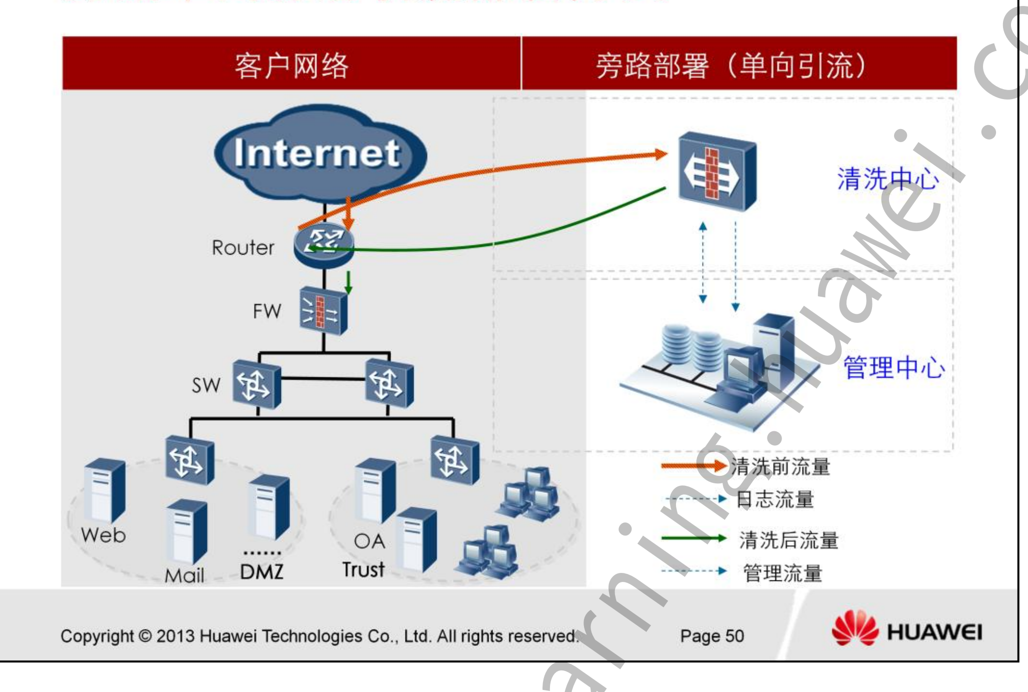




HUAWEI

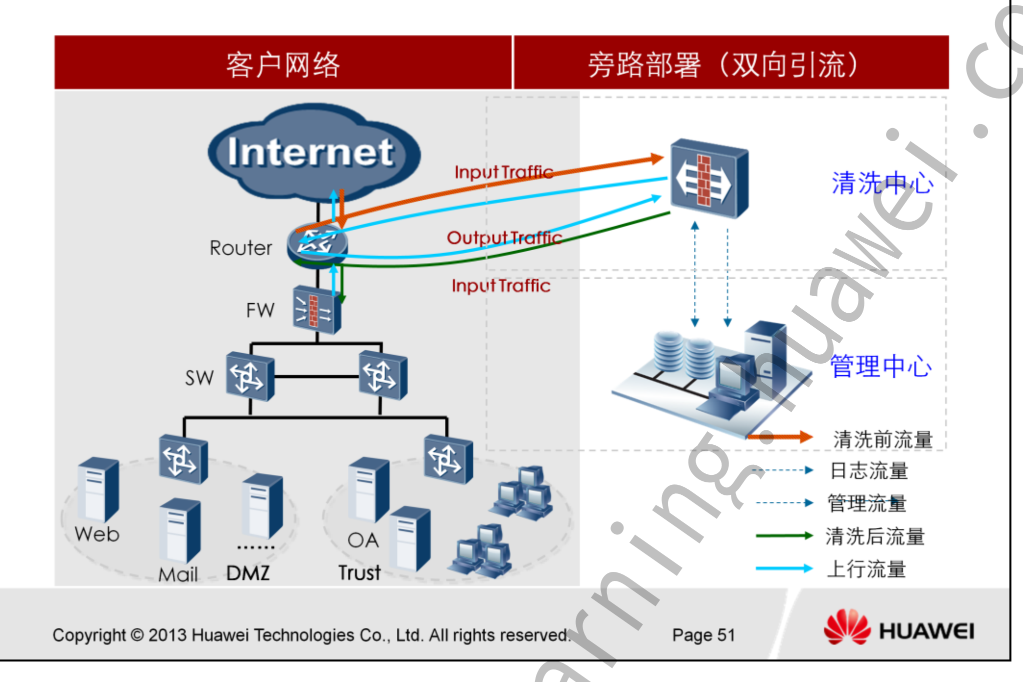
将清洗设备直路部署在客户网络中，如果对可靠性要求高，可以部署主备方式及Bypass模块，提供最佳可靠性。

清洗设备也是根据管理中心配置的防御策略对网络流量进行清洗。清洗中心将业务日志发送到管理中心，形成各类报表。




单向引流指仅引流进入防护网络的流量，基于单向流量进行外部攻击防御。可使用策略路由或者动态路由引流。

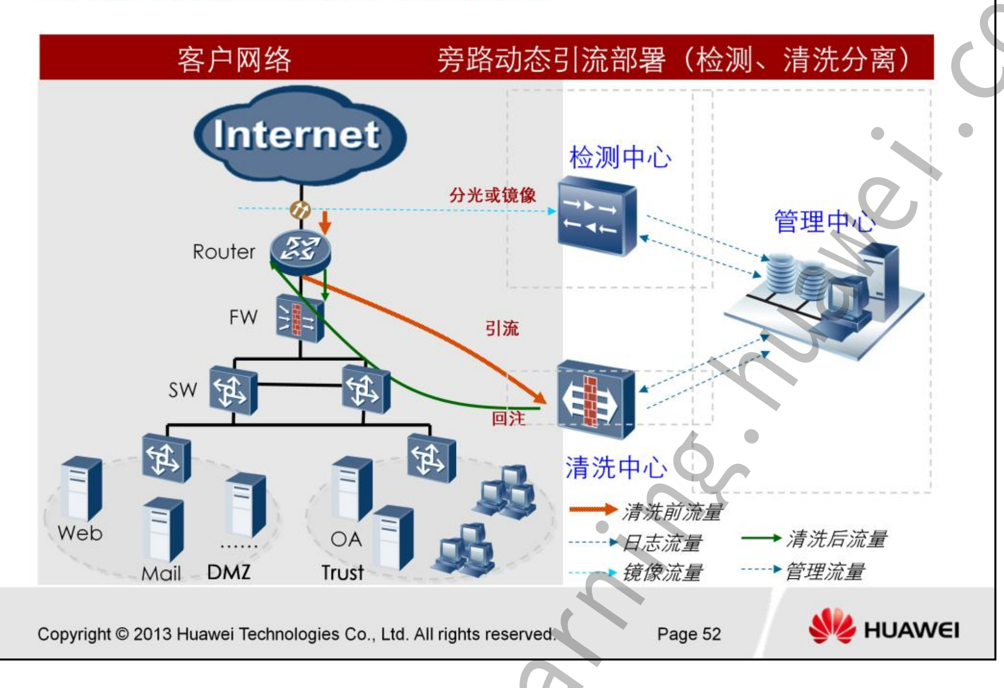
将清洗设备旁路部署在网络出口，通过路由将到流入防护网络的流量引流至清洗设备进行清洗，清洗后的流量回。清洗中心业务日志发送到管理中心，形成各类报表。




下行引流方式：策略路由引流。上行引流方式：策略路由引流、高优先级默认路由引流。这是一种逻辑直路的部署方式，相比于单向引流，这种来回路径一致的部署方式可以提供全面的防范和较高可靠性。

清洗设备旁路部署在网络出口，通过路由将防护网络流入及流出流量均引流至清洗设备，基于来回路径一致对流入流量进行检测和清洗，清洗后的流量回注入网络中。

双向引流引入流入及流出两个方向的流量，可基于会话等信息更加准确的对攻击进行防御；同时华为基于多核处理器的硬件平台，保证了防御的高性能。




- **镜像方式**
  - 通过1：2或者1：3分光方式引入检测中心设备；
  - 在出口设备上使用端口镜像方式引入检测中心设备。
- **引流方式**
  - 策略路由静态引流；
  - BGP动态引流。
- **回注方式**
  - 策略路由回注；
  - 使用VPN回注，可选MPLS VPN、GRE VPN等方式回注；
  - 路由回注，如使用静态路由或者默认路由回注。

镜像、引流、回注方式需要综合现网情况灵活选取。将清洗/检测设备旁路部署在网络出口，将防护网络的下行流量镜像至检测设备；管理中心根据检测结果通知清洗设备进行有引流和清洗。用户可灵活控制引流及清洗过程。



# 目录









# 引流方案

引流方案一般针对于旁路部署且为动态引流方案。对城域网而言，在城域网入口设备上引流，对于扁平化网络，城域网入口设备兼汇聚设备，采用动态路由引流时会导致回注方案复杂化。

| 引流方法 | 描述 | 优点 | 缺点 | 可选回注方法 |
| --- | --- | --- | --- | --- |
| 动态路由引流 | 利用BGP协议动态引流 | 动态引流，无需人工干预 | 回注方法复杂，不能再使用路由方式将流量回注到原来的引流点。 | MPLSVPN隧道方式<br>GRE隧道方式<br>策略路由方式 |
| 静态策略路由引流 | 手工配置策略路由，将流量引向清洗设备 | 无需布署BGP路由协议，回注方案简单 | 容易将大流量引入到清洗设备，增加网络延迟。 | 路由方式<br>MPLSVPN隧道方式<br>GRE隧道方式<br>策略路由方式 |
| 静态路由引流 | 手工配置长掩码的静态路由，将流量引向清洗设备 | 无需布署BGP路由协议 | 回注方法复杂，不能再使用路由方式将流量回注到原来的引流点。 | MPLSVPN隧道方式<br>GRE隧道方式<br>策略路由方式 |





# 回注方案

旁路部署的情况下，需要将流量回注到原有网络中，回注方式对比如下：从网络适应性和配置难易程度来看，推荐使用策略路由回注。

| 回注方法 | 描述 | 优点 | 缺点 | 适用网络 |
|---|---|---|---|---|
| 策略路由方式 | 使用策略路由回注 | 不依赖与路由协议 | 配置复杂，需要在回注的多个转发路径上配置策略路由，难以处理有备份链路和负载分担链路的情况 | 适合所有网络 |
| MPLSVPN隧道方式 | 通过MPLS VPN隧道回注流量 | | 布署复杂，需要设备支持MPLS VPN功能，配置的设备较多 | 不适合扁平化组网 |
| 路由方式 | 使用普通路由回注流量 | 布署简单 | 使用路由方式引流后无法再使用路由方式回注，否则会形成回路 | 适合所有网络 |
| GRE隧道方式 | 通过GRE隧道回注流量 | 布署简单 | 需设备支持GRE隧道功能 | 不适合扁平化组网 |





# 引流与回注的组合方法

引流回注方法组合方式如下：

| | 路由回注 | 策略路由回注 | MPLS VPN回注 | GRE隧道回注 | 二层回注 |
|---|---|---|---|---|---|
| 动态路由引流 | 无法组合 | 推荐使用 | 可以组合 | 可以组合 | 无法组合 |
| 静态路由引流 | | | | | 无法组合 |
| 静态策略路由引流 | 可以组合 | 推荐使用 | 可以组合 | 可以组合 | 可以组合 |









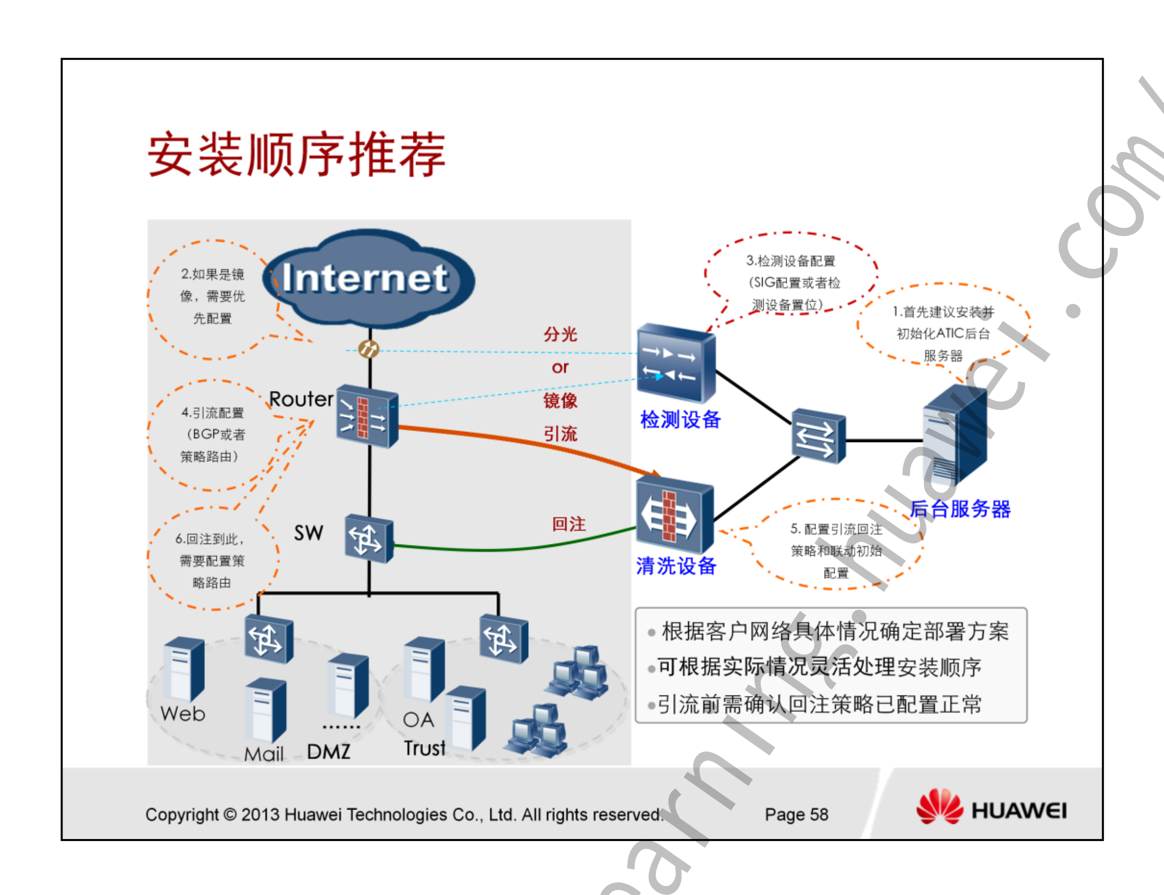
# 目录





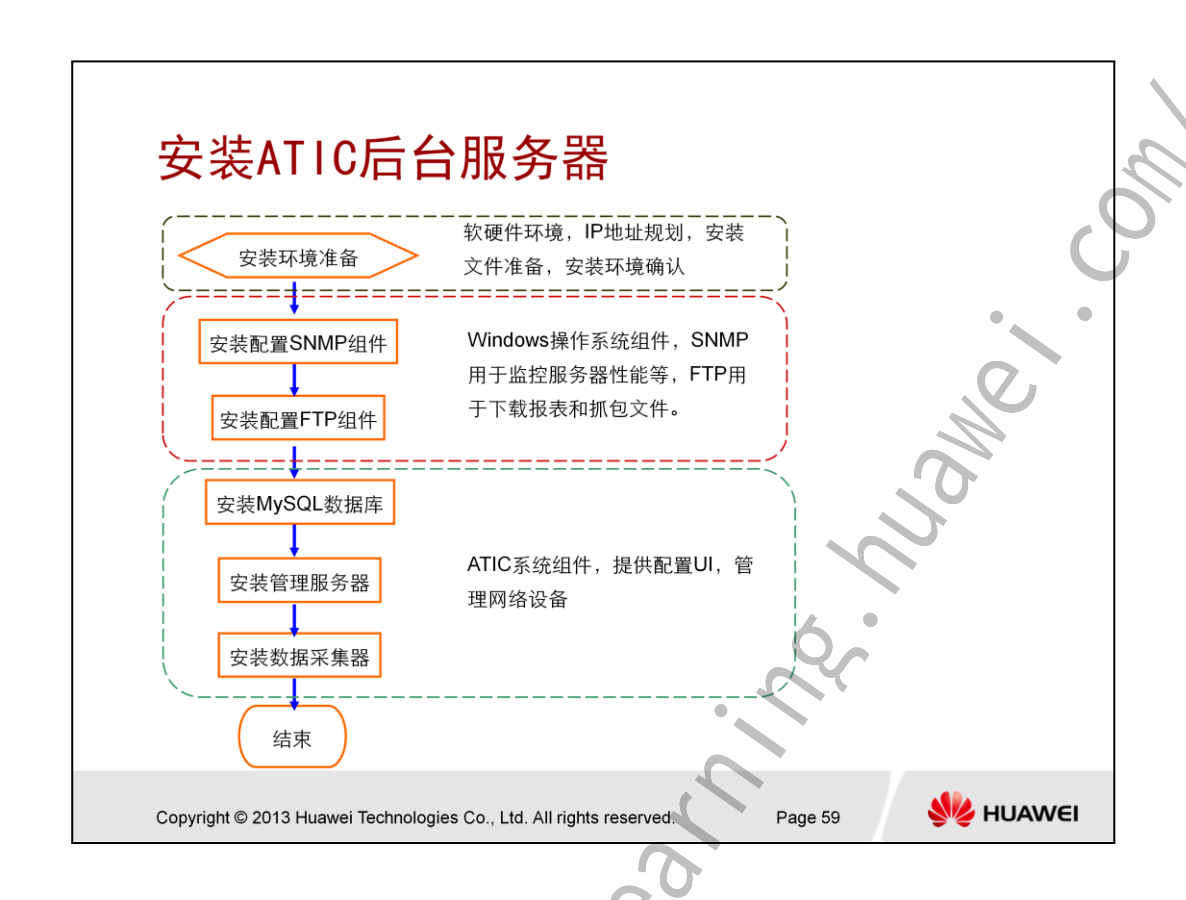







- **镜像方式:**
  - 通过1: 2或者1: 3分光方式引入检测中心设备;
  - 在出口设备上使用端口镜像方式引入检测中心设备。
- **引流方式:**
  - 策略路由静态引流;
  - BGP动态引流。
- **回注方式:**
  - 策略路由回注;
  - 使用VPN回注，可选MPLS VPN、GRE VPN等方式回注;
  - 路由回注，如使用静态路由或者默认路由回注。

镜像、引流、回注方式需要综合现网情况灵活选取。




简单介绍ATIC管理中心在整个异常流量监管方案中的地位和主要功能。

ATIC（Abnormal Traffic Inspection & Control System）管理中心是异常流量监管（DDoS防御）方案的中枢，通过管理中心将检测中心和清洗中心连接起来形成完整的异常流量监管方案。

ATIC管理中心的主要功能包括下面几项：

- 统一管理和监控检测设备和清洗设备；
- 统一管理大客户信息，配置大客户防御策略；
- 接收检测分析中心的检测结果，进行汇总分析；
- 根据检测结果制定引流防御策略，下发到清洗设备；
- 接收清洗设备的上报信息，进行汇总分析；
- 根据全面的分析数据，形成统计报表。

# 配置出口核心设备

出口核心设备主要是配置引流方式和端口镜像。在处理路由的时候需要高度注意，避免引起路由环路。

| 关键配置项 | 条件 | 建议 |
|---|---|---|
| 端口镜像 | 电接口，无光链路不使用分光方式 | 将下行流量镜像到检测设备即可 |
| BGP | 需要旁路动态引流情况下 | 与清洗设备建立eBGP邻居 |
| 策略路由 | 1.旁路静态引流<br>2.引流回注为同一台设备 | 引流回注为同一台设备时候，需要使用策略路由将数据包发往下行网络，否则会形成环路 |







# 配置检测清洗设备

| 关键配置项 | 条件 | 建议 |
| --- | --- | --- |
| 配置与清洗设备联动 | SIG作为检测设备 | 只需配置大客户参数 |
| 配置检测设备 | Anti-DDos8000检测板检测 | 配置为检测板即可 |
| | Anti-DDos1000检测 | 必须独立使用，无法混插 |
| 配置引流 | 动态引流 | 建立eBGP邻居 |
| | 策略静态引流 | |
| 配置回注 | 必需 | 推荐使用策略路由回注 |
| 开启流量统计 | 必需 | 在引流口配置 |
| 配置远程管理 | 必需 | ATIC需通过telnet或SSH下发命令。 |







配置检测设备

回注路由器之间建立MPLS L3VPN，将清洗后的流量通过MPLS L3VPN回注到原链路，最后送到防护对象。 Anti-DDos8000检测板检测

在用户视图下执行命令system-view，进入系统视图。

执行命令firewall ddos { detect-spu | clean-spu } slot slot-id，指定槽位业务板为检测业务板或清洗业务板。 保证已经导入License的前提。

使用检测设备AntiDDoS1500-D

# ATIC系统配置操作步骤介绍

新老版本的ATIC系统登录方式不同

- 老版本登录ATIC管理页面 https://atic-server-ip/atic
- 新版本的登录方式 http://atic-server-ip

新版本有两种方式管理ATIC

- 通过VSM的ATIC管理组件管理DDOS系统
- 独立安装ATIC业务管理组件管理DDOS系统

缺省用户名/口令不变 admin / Admin@123

其配置界面相同




ATIC系统配置分为网络设备配置和ATIC服务器配置，首先登录网络设备配置接口IP、工作模式和登录账号，然后登录ATIC服务器配置网络设备和防御对象及防御策略。

## 配置网络设备

- 配置系统参数
- 开启Telnet/SSH服务
- 配置SNMP功能
- 配置逻辑接口
- 配置检测设备的接口功能
- 配置清洗设备的接口功能
- 配置混插设备的接口功能
- 指定检测或清洗业务板
- 配置链路状态检测功能
- 配置信息同步功能






配置系统参数：系统参数配置是指设备上电成功后，系统调测配置。包括语言模式、设备名称、系统时间、登录提示信息和命令行级别的配置；

开启Telnet/SSH服务：开启Anti-DDoS设备的Telnet功能或SSH功能，其他设备可以通过这种方式远程登录到Anti-DDoS设备；

配置SNMP功能：通过配置SNMP功能，使管理中心可以获取Anti-DDoS设备的状态；

配置逻辑接口：介绍Eth-Trunk和Loopback接口的配置；

配置检测设备的接口功能：当检测设备作为Anti-DDoS设备独立部署时，需要按照本节配置各种接口功能；

配置清洗设备的接口功能：当清洗设备作为Anti-DDoS设备独立部署时，需要按照本节配置各种接口功能；

配置混插设备的接口功能：当混插设备作为Anti-DDoS设备独立部署时，需要按照本节配置各种接口功能；

指定检测或清洗业务板：缺省情况下，业务板类型为防火墙业务板，不具有检测或清洗功能，用户需指定某槽位业务板为检测业务板或清洗业务板；

配置链路状态检测功能：链路状态检测功能用于报文来回路径一致组网中的链路状态合法性检查，如TCP连接状态等；

配置信息同步功能：当检测设备与清洗设备分别作为独立设备旁路部署时，配置信息同步功能后检测设备上一些关键状态信息可以同步到清洗设备。

# 配置ATIC服务器

配置和业务部署相关的内容主要集中在资源和业务两个菜单里

- 在ATIC管理页面里的资源菜单里添加网络设备和采集器；
- 在业务菜单里添加防御对象和防御策略。



# ATIC配置步骤-网元发现&添加采集器

- 点击资源>发现策略>创建，选用一种方式发现网元设备；
- 点击资源>采集器管理>创建，添加采集器。










# 使用配置向导

在业务>快速入门 里使用配置向导，按顺序点击相应图标即可进入相应配置页面，完成配置后，需重新进入快速入门里选择下一步配置图标，进行下一步配置。





# 总结

- 常见DDoS攻击技术
- DDOS攻击防范方案
- DDOS攻击防范组网







## 思考题

- 什么是DDOS攻击?
- DDoS攻击有哪些分类?
- 各DDOS攻击实现原理有何不同，及相应防范技术是什么?
- 异常流量清洗解决方案由哪些组件组成?
- 异常流量清洗解决方案有哪些组网方式?
- 异常流量清洗解决方案是如何进行引流和回注?








# 练习题

- 判断题

  1. 异常流量清洗解决方案既支持旁路部署又支持直路部署。

- 多选题

  1. 异常流量清洗解决方案主要由以下哪些组件组成?

  A. 管理中心　B. 采集中心　C.检测中心　D.清洗中心








习题与答案：

1、异常流量清洗解决方案既支持旁路部署又支持直路部署。

答案：正确

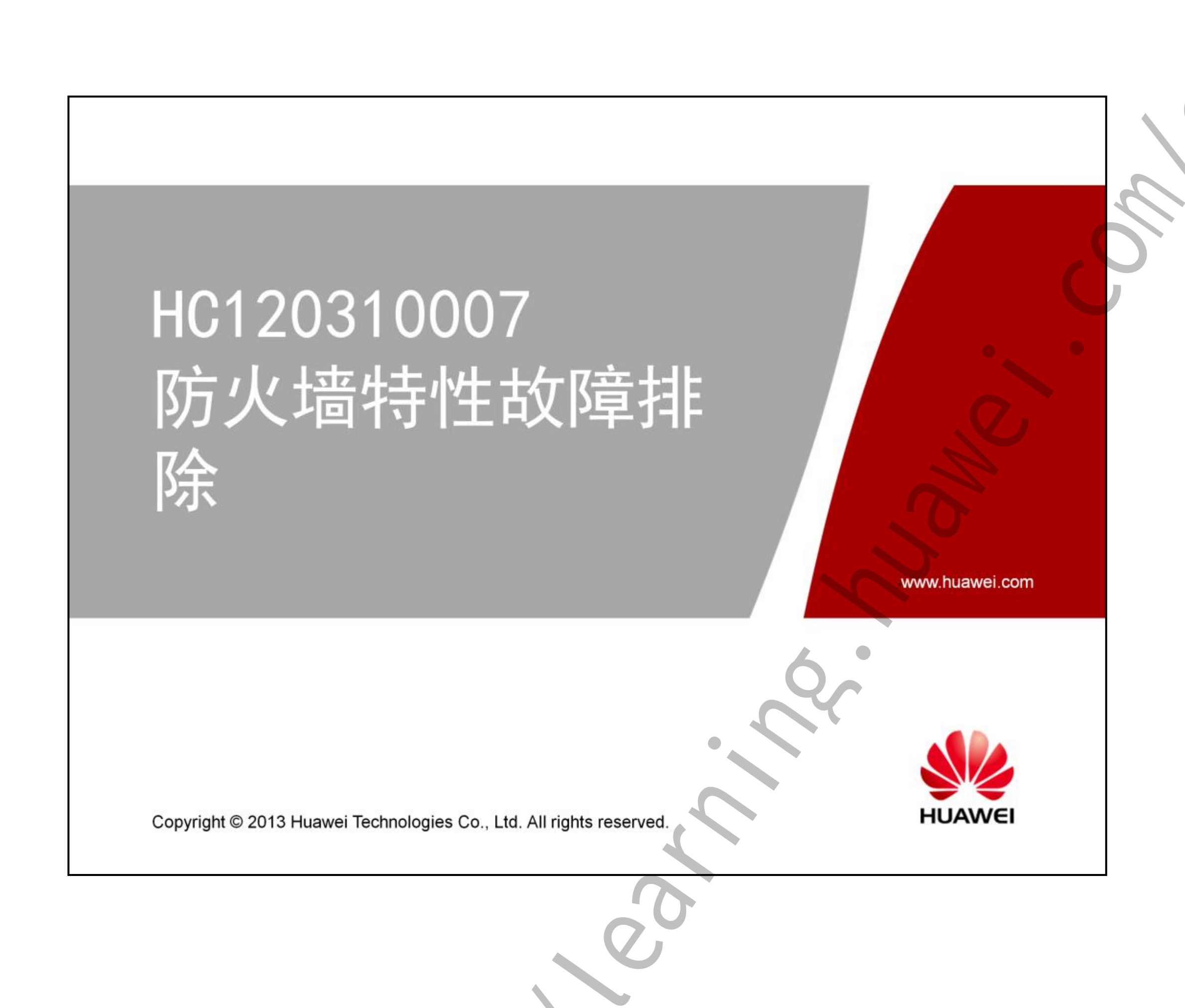
2、异常流量清洗解决方案主要由以下哪些组件组成?

A. 管理中心　B. 采集中心　C. 检测中心　D. 清洗中心

答案：A|C|D

Thank you

www.huawei.com


HC120310007
防火墙特性故障排除
www.huawei.com
HUAWEI



# 目标

- 学完本课程后，您将能够:
  - 掌握故障处理方法
  - 掌握安全策略故障排除
  - 掌握防火墙高级安全特性故障排除
  - 掌握双机热备故障排除
  - 掌握L2TP VPN故障排除
  - 掌握IPSEC VPN故障排除
  - 掌握SSL VPN故障排除








# 目录

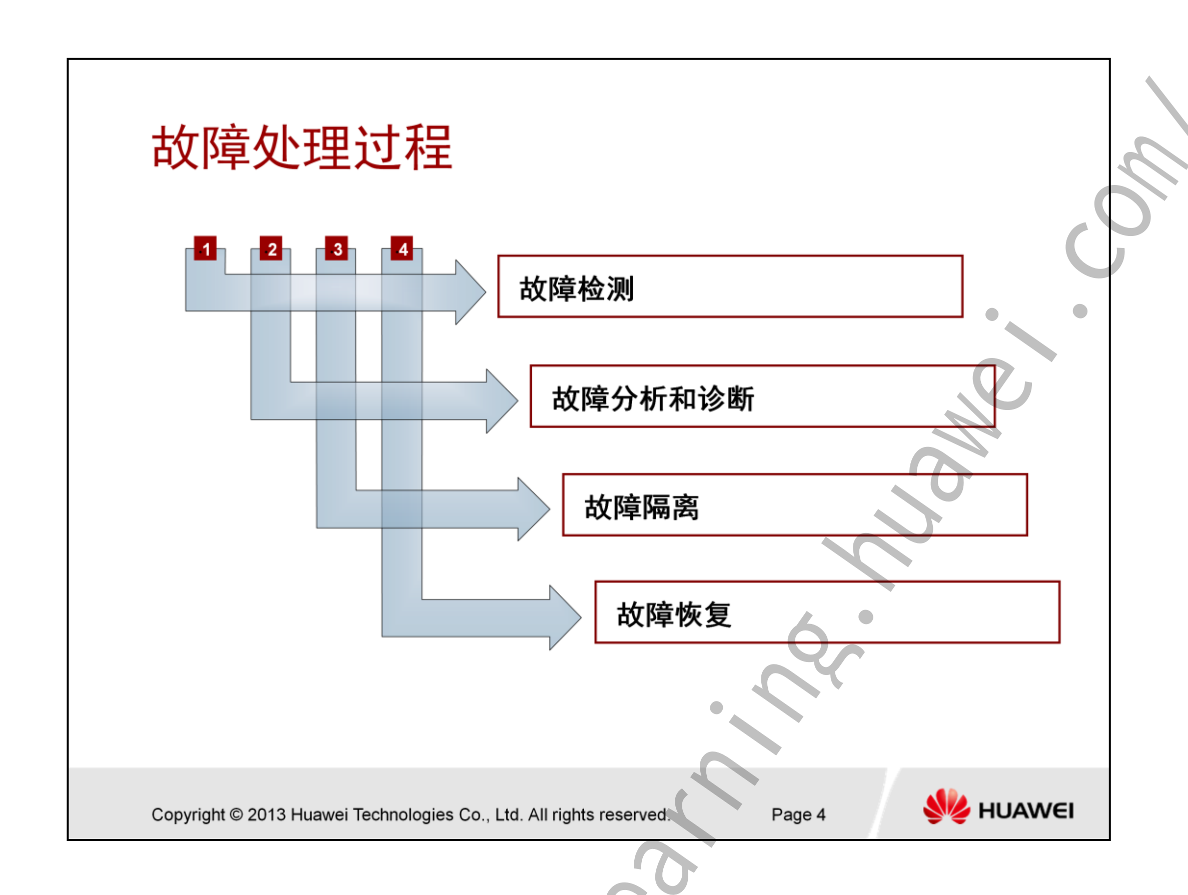













故障管理过程包括对故障现象进行检测和分析，从而对故障进行隔离，直到最后隔离或解决故障。

故障检测：主要是观察故障现象，检查数值范围、数据正确性，对同类型的多个输出进行比较检查，对心跳检测进行分时段检查等。

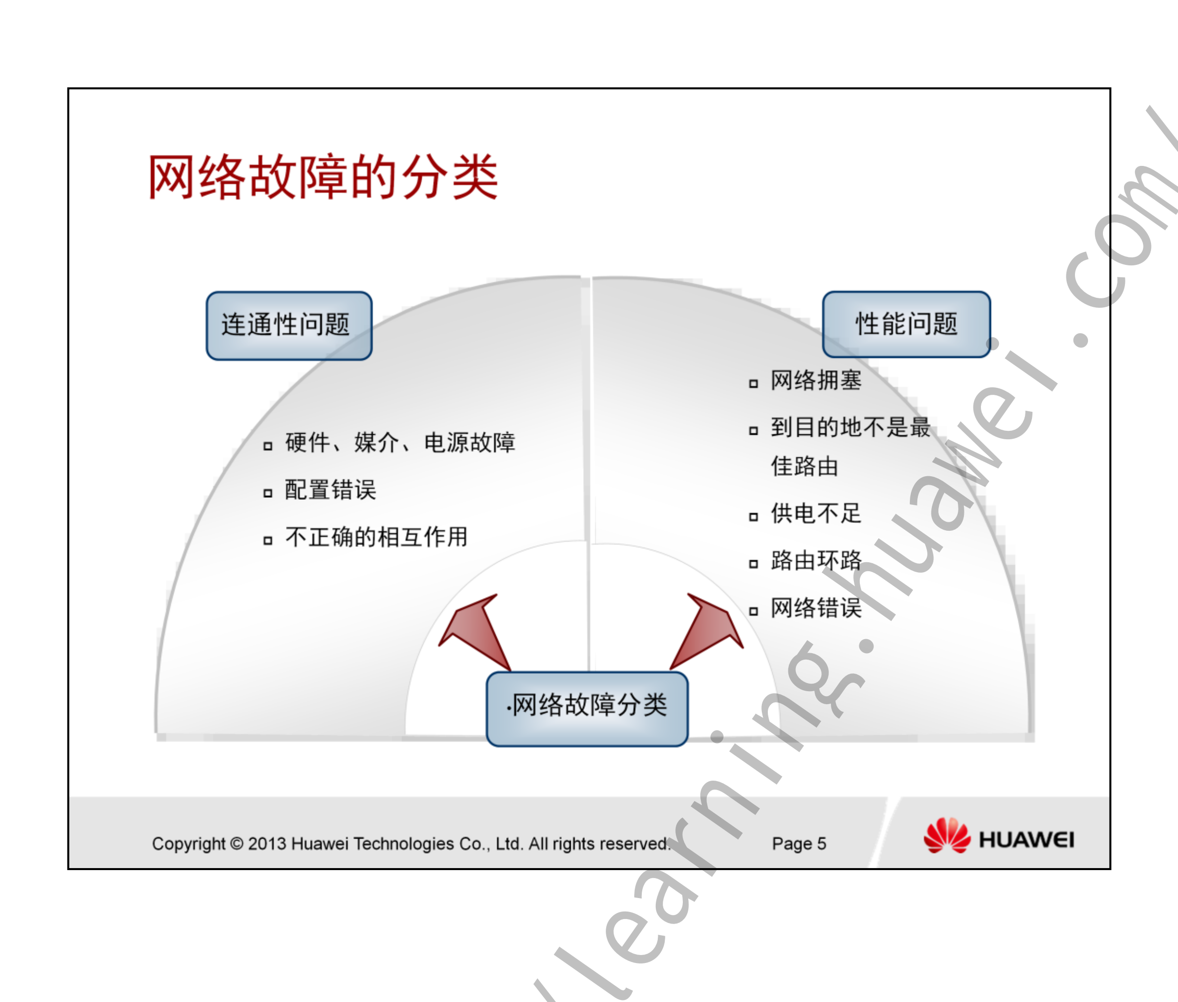
故障分析和诊断：主要是采用各种故障分析方法，通过调试工具进行分析，从而确定故障发生的具体位置。

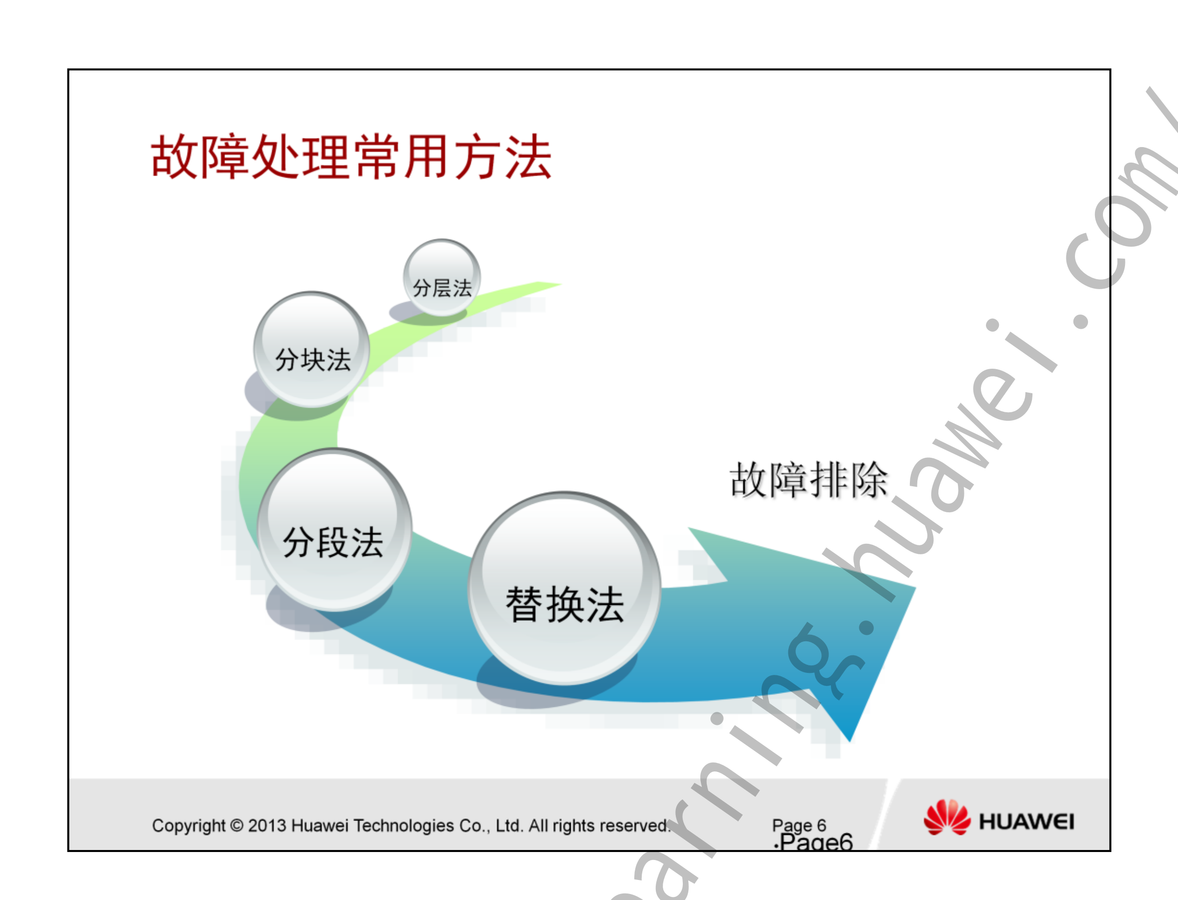
故障隔离：主要是把检测到的故障单元（或模块）隔离到待修理范围的过程。例如拔出故障单板，禁止故障功能单元工作，调整参数范围，修改转发表项，或重选路由等。

故障恢复：主要是让设备暂时恢复到正常执行功能的过程。例如通过执行软件复位或重启。

故障彻底解决：主要是让设备彻底摆脱故障。例如更换故障单元，对软件进行补丁和升级。

故障检测和分析是解决故障的前提，分析方法随着时间和空间有不同特点，因此需要针对不同网络环境采取针对性的分析方法，从而高效地发现故障。


网络故障的分类
连通性问题
硬件、媒介、电源故障
配置错误
不正确的相互作用
性能问题
网络拥塞
到目的地不是最佳路由
供电不足
路由环路
网络错误
网络故障分类
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 5
HUAWEI


故障处理常用方法
分层法
分块法
分段法
替换法
故障排除
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 6
HUAWEI

# 分层处理法思想

当模型的所有低层结构工作正常时，它的高层结构才能正常工作

| | 物理层 | 数据链路层 | 网络层 |
|---|---|---|---|
| 主要功能 | ▫通过某种介质提供到另一设备的物理连接<br>▫进行端点间二进制流的发送与接收<br>▫完成与数据链路层的交互操作 | ▫在网络层与物理层之间进行信息传输<br>▫规定介质如何接入和共享<br>▫规定如何对站点进行标识<br>▫规定如何根据物理层接收的二进制数据建立帧 | ▫对数据进行分段、打包、重组；<br>▫发送差错报告；<br>▫寻找通过网络的最佳路径来发送信息 |
| 排错思路 | ▫关注因素包括：电缆、连接头、信号电平、编码、时钟、组帧方式。 | ▫封装不一致，如display interface显示端口物理状态是up而协议状态是down，则数据链路层存在故障<br>▫链路的利用率，如链路带宽被过度使用 | ▫地址错误和子网掩码错误<br>▫因特网络中的地址重复<br>▫路由协议错误 |

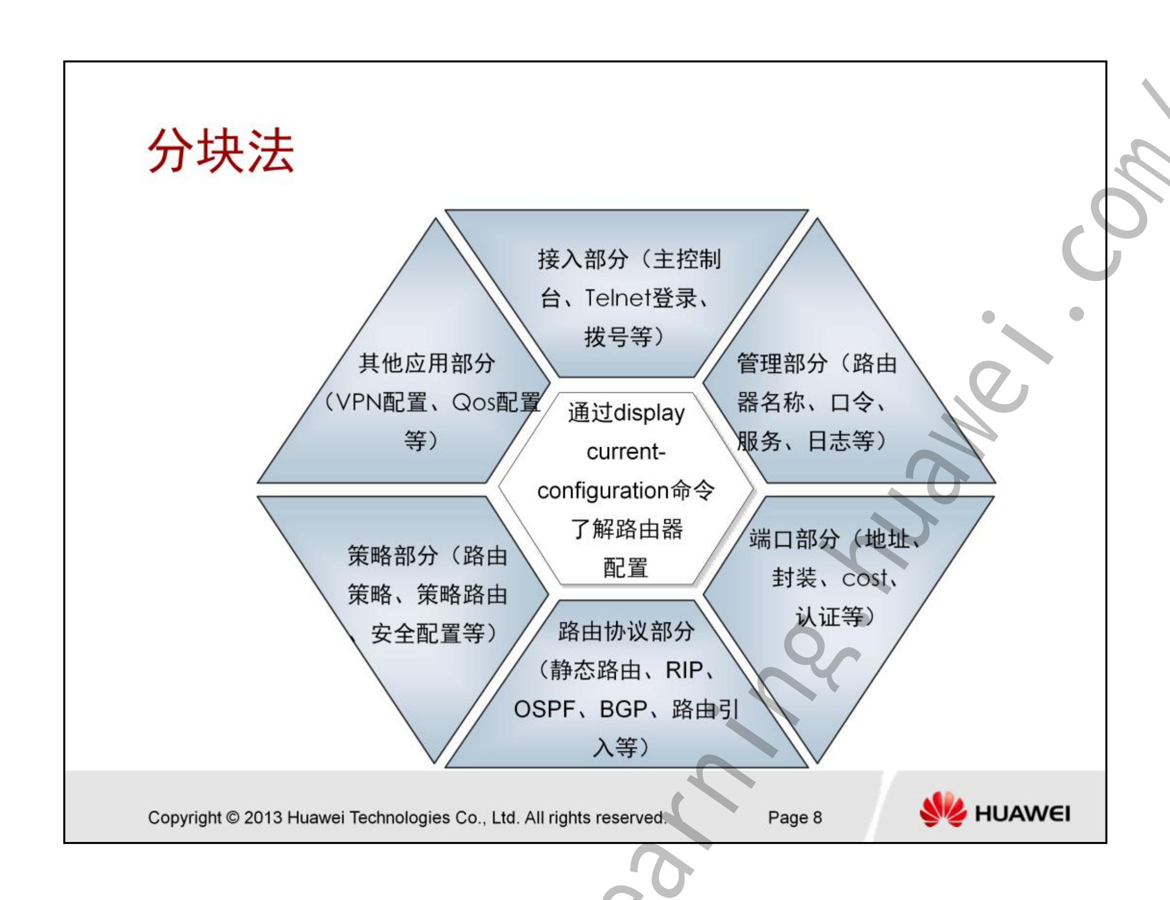


HUAWEI

排除网络层故障的基本方法是：

沿从源节点到目的节点的路径，查看各路由器上的路由表，同时检查这些路由器接口的IP地址。

通常，如果路由没有在路由表中出现，应该检查是否已经配置了正确的静态路由、缺省路由或动态路由，如果不是，手工配置丢失的路由或排除动态路由协议故障使路由表更新。




例如：执行display ip routing-table命令，显示结果中只包含直连路由，那么问题可能发生在哪里呢？

从上述的配置文件分块中可以看到，有三类原因可能引起该故障：

路由协议：如果没有配置路由协议或配置不当，路由表可能为空；

策略：如果访问列表配置错误，可能导致路由不能正常更新；

端口：如果端口的地址、掩码或认证配置错误，也可能导致路由表错误。

# 分段法

将大的网络拆分成小段分别排查

主机到路由器/交换机的LAN接口

路由器/交换机到防火墙接口

防火墙到电信部门接口

WAN电路

防火墙本身或路由器/交换机本身

故障排除






替换法
替换法是判断硬件故障时最常用的方法。
怀疑故障的单板或设备
正常的单板或设备
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 10
HUAWEI



# 目录









# 故障处理方法

**查看状态**

- 查看配置文件
- 查看设备状态
- 查看协议表项

**测试命令**

- Ping，Tracert测试报文从发送主机到目的地所经过的网关，主要用于检查网络连接是否可达，以及初步定位网络发生故障的位置。

**告警与日志**

- 当设备发生故障或系统工作状态异常时，系统能够产生告警信息。
- 介绍日志信息的分类以及输出方式、告警信息的显示。

**抓包功能和Debug工具**

- 抓包是一种将通过设备的数据报文捕获到PC上的方法，通过分析抓到的包可以详细了解数据包的实际内容。







VRP平台ping介绍

ping [ -a source-ip-address | -c count | -s packetsize | -t timeout ] * host

-a source-ip-address：设置发送ICMP Echo Request报文的源IP地址。

-c count：设置发送ICMP Echo Request报文的次数，缺省值为5。

-s packetsize：设置发送ICMP Echo Request报文的长度（不包括IP和ICMP报文头），以字节为单位，缺省值为56。

-t timeout：设置ping报文的超时时间，缺省值为2000ms。

VRP平台tracert介绍

tracert [ -a source-ip-address | -f first-TTL | -m max-TTL | -p port | -q nqueries | -w timeout ] * host

-a source-ip-address：设置tracert报文的IP地址。

-f first-TTL：设置初始TTL。

host：目的主机的IP地址。

# 查看配置文件

- 通过display相关命令检查配置文件的信息。
- 在日常维护工作中，可以在任意视图下选择执行以下命令，查看配置文件信息。
- 查看配置文件信息的相关操作
  - 查看当前配置文件
    - display current-configuration
  - 查看设备下次启动时加载的配置文件的内容
    - display saved-configuration





# 查看设备信息

- 查看版本信息
  通过display version命令可以获取设备软件运行版本、BootROM版本及各种存储器的大小。故障设备使用的系统软件的版本是进行定位的重要信息。
- 查看接口信息
  通过display interface/display ip interface等命令可以查看接口的状态信息。常用于设备接口对接故障、查看报文丢包统计。
- 查看硬件状态信息
  通过display device/display environment命令可以查看设备各部件（主控板、单板、风扇、电源等）的运行状态及内存CPU的使用率，通常在硬件发生故障时使用。






# 查看会话表

- 查看会话表简要信息
- 通常使用display firewall session table命令查看所有的会话的简要信息。

- 查看会话表详细信息
- 通常使用display firewall session table verbose命令可以查看会话表的详细信息，如存活时间、下一跳接口、该会话的字节数统计等。








**查看会话表简要信息**

通常使用**display firewall session table**命令查看所有的会话的简要信息。

<sysname> **display firewall session table** Current Total Sessions : 4 icmp VPN:public --> public Remote 192.168.1.1:43985-->192.168.2.2:2048 telnet VPN:public --> public 192.168.3.1:2855-->192.168.3.2:23 netbios-name VPN:public --> public 192.168.3.4:137-->192.168.3.255:137 http VPN:public --> public 192.168.3.8:2559-->192.168.3.200:80

**查看会话表详细信息**

通常使用**display firewall session table verbose**命令可以查看会话表的详细信息，如存活时间、下一跳接口、该会话的字节数统计等。

<sysname> **display firewall session table verbose** Current Total Sessions : 1 telnet VPN:public --> public TTL: 00:10:00 Left: 00:10:00 Interface: InLoopBack0 NextHop: 127.0.0.1 MAC: 00-00-00-00-00-00 <--packets:1269 bytes:66769 -->packets:1081 bytes:43715 128.18.196.6:2855-->128.18.196.200:23

## Ping与Tracert

- Ping命令用于检查网络连接及主机是否可达。Tracert命令用于测试数据报文从发送主机到目的地所经过的网关。
- Ping简介
  - Ping命令主要用于检查网络连接及主机是否可达。
- Ping命令格式
  - ping [ ip ] [ -a source-ip-address | -c count | -f | -s packetsize | -t timeout ]* host







**Ping简介**

Ping命令主要用于检查网络连接及主机是否可达。Ping功能是基于ICMP协议来实现的：源端向目的端发送ICMP回显请求（ECHO-REQUEST）报文后，根据是否收到目的端的ICMP回显应答（ECHO-REPLY）报文来判断目的端是否可达。对于可达的目的端，再根据发送与接收报文个数、Ping报文的往返的响应时间来判断链路的质量。

**Ping命令格式**

命令参考手册提供了命令的详细使用方法，这里只对常用的参数进行解释说明。

**ping** [ **ip** ] [ **-a** *source-ip-address* | **-c** *count* | **-f** | **-s** *packetsize* | **-t** *timeout* ]* *host*

-a：设置发送ECHO-REQUEST报文的源IP地址，通常在测试VPN时使用。

-c：发送ECHO-REQUEST报文的次数，缺省为5。

-f：设置发送的报文不分片，中间如果MTU值小于报文大小会丢弃该报文。

-t：为发送完ECHO-REQUEST后，等待ECHO-RESPONSE的超时时间。在网络状况不好的情况下，可以适当改大该参数。缺省为2s，即2s内没有收到回复报文即认为目的不可达。

-s：设置报文大小（不含IP和ICMP头）。

host：可以是IP地址或域名，如果是域名会首先进行DNS解析，并显示解析后的IP地址。

## Ping与Tracert

- Tracert简介
- ping可以告诉用户目标是否可达，而tracert命令用于测试数据包从发送主机到目的地所经过的设备，它主要检查网络连接是否可达，以及分析网络什么地方发生了故障。
- Tracert命令格式
- tracert [ -a source-ip-address | -f first-ttl | -m max-ttl | -p port | -q nqueries | -vpn-instance vpn-instance-name | -w timeout ] * host
- -a：指明本次tracert命令配置的报文源地址
- -w：等待响应报文的超时时间。






Tracert命令格式

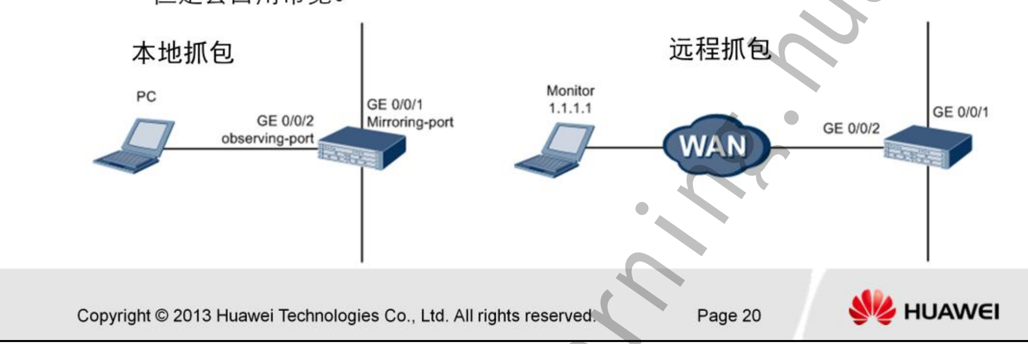
tracert [ -a source-ip-address | -f first-ttl | -m max-ttl | -p port | -q nqueries | -vpn-instance vpn-instance-name | -w timeout ] * host

-a：指明本次tracert命令配置的报文源地址

-w：等待响应报文的超时时间。

## 抓包功能

- 抓包是一种将通过设备的数据报文捕获到PC上的方法，通过分析抓到的包可以详细了解数据包的实际内容。
    - 本地抓包：将负责解析的PC直接连接在设备的以太网口上。这种方式对网络冲击较少，需要PC直连设备。
    - 远程抓包：设备将内容发送到远端的PC上。要求设备与PC互通即可，但是会占用带宽。




- 本地抓包:

  设备上配置观测口（与PC直连的接口），端口镜像功能会将被监控口的数据复制到该接口。

  [sysname] observing-port GigabitEthernet 0/0/2

  设备上配置镜像口（待监控的接口）

  [sysname] port-mirroring GigabitEthernet 0/0/1 both GigabitEthernet 0/0/2

- 远程抓包:

  定义要抓包的范围，这里以抓所有源地址为192.168.1.0网段的报文为例。

  [sysname-acl-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255

  如下命令配置将符合acl3000的所有经过接口的IPv4报文放入发送队列中。

  [sysname] packet-capture ipv4-packet 3000 interface GigabitEthernet 0/0/1

  启动抓包功能。

  [USG] packet-capture startup manual

  将指定抓包队列保存为1.cap文件到设备上，默认存放盘符是hda1。

  [USG] packet-capture queue 0 to-file 1.cap

  用户通过FTP服务从设备上下载1.cap文件，使用抓包软件打开。

# Debugging

- 执行命令terminal monitor，启用终端显示信息功能。
  - 缺省情况下，未启用控制台或终端的显示信息功能。该命令只对当前输入命令的终端有效。
- 执行命令terminal debugging，启用终端显示Debugging信息功能。
  - 缺省情况下，未启用控制台或终端显示Debugging信息功能。
- 打开调试开关
  - Debugging [Protocol]








# 目录









# 安全策略导致业务不通故障排除思路

包过滤场景故障

1. ACL配置错误
   - 规则配置错误
   - 规则顺序配置错误
2. 域间应用错误
   - 域间选择错误
   - 域间方向错误







# 原因一：ACL配置错误

- 执行命令display policy interzone，查看ACL配置：

```
<USG> display policy interzone untrust trust inbound
policy interzone trust untrust inbound
 firewall default packet-filter is deny
 policy 0 (2478 times matched)
  action deny
  policy service service-set ip
  policy source any
  policy destination any
 policy 1 (0 times matched)
  action permit
  policy service service-set ip
  policy source 1.1.1.0 0.0.0.255
  policy destination 2.2.2.0 0.0.0.255
```







检查规则中的源、目的或源端口、目的端口配置是否有误。规则的执行顺序为：policy按照先后顺序依次执行，默认域间策略最后执行。默认情况下号码小的排在前面，但是可以通过policy move命令来调整顺序(号码保持不变)。

# 原因二：域间应用错误

- 执行命令display policy interzone，查看域间包过滤情况：

```
<USG> display policy interzone untrust trust inbound
policy interzone trust untrust inbound
 firewall default packet-filter is deny
 policy 0 (0 times matched)
  action permit
  policy service service-set ip
  policy source 1.1.1.0 0.0.0.255
  policy destination 2.2.2.0 0.0.0.255
policy 1 (2478 times matched)
  action deny
  policy service service-set ip
  policy source any
  policy destination any
```

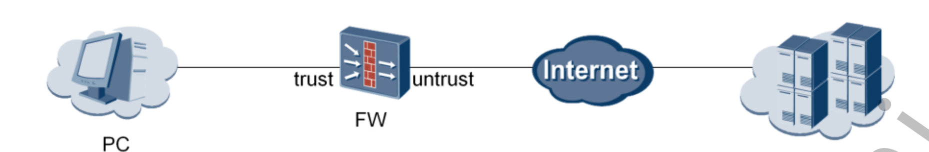







根据流量经过防火墙的两个接口所在的域，选择在合适的域间应用规则。根据各安全域的安全级别及包过滤的源、目的地址段，选择合理的域间方向。

# 案例：包过滤配置问题导致网页打开慢







- 故障现象
  - PC通过NAT Outbound访问Web Server；
  - 通过精确的ACL严格控制PC可访问的Web Server地址范围；
  - 访问部分网站速度慢，有时打开一个网页需要20多秒。

# 案例：包过滤配置问题导致网页打开慢

- 原因分析

| 2011-02-21 15:33:46.071855 | 172.20.21. | 218.200.227. | HTTP | GET /html/js/byslidem.js HTTP/1.0 |
|---|---|---|---|---|
| 2011-02-21 15:33:46.210820 | 172.20.21. | 218.200.227. | HTTP | GET /html/js/bysliden.js HTTP/1.0 |
| 2011-02-21 15:33:46.286713 | 172.20.21. | 218.200.227. | HTTP | GET /html/js/window.js HTTP/1.0 |
| 2011-02-21 15:34:07.381124 | 172.20.21. | 218.200.227. | HTTP | GET /html/js/search/thickbox-compressed.js HTTP/1.0 |
| 2011-02-21 15:34:07.537001 | 172.20.21. | 218.200.227. | HTTP | GET /html/js/search/jquery.autocomplete.min.js HTTP/1. |
| 2011-02-21 15:24:41.489012 | 172.20.36.83 | 218.200.227. | HTTP | GET /html/js/window.js HTTP/1.0 |
| 2011-02-21 15:24:41.636090 | 172.20.36.83 | 203.208.39. | HTTP | GET /ga.js HTTP/1.0 |
| 2011-02-21 15:24:41.979063 | 172.20.36.83 | 218.200.227. | HTTP | GET /html/js/search/thickbox-compressed.js HTTP/1.0 |

- 解决方法
  - 将ga.js文件所在的IP地址203.208.39.XX加入到ACL的运行范围。








原因分析

在出现问题的PC上抓包：可以看到PC在请求完window.js后，过了21秒才去请求下一个文件thickbox-compressed.js，问题应该就在这里；

绕过FW在访问正常的PC上抓包：发现PC请求window.js和thickbox-compressed.js之间还请求了ga.js文件，而这个文件所在地址发生了变换，并且变换后地址并不在ACL允许范围，所以PC多次请求203.208.39.XX地 址ga.js文件没有结果后，转向其他IP请求其他文件，从而导致网页打开慢。



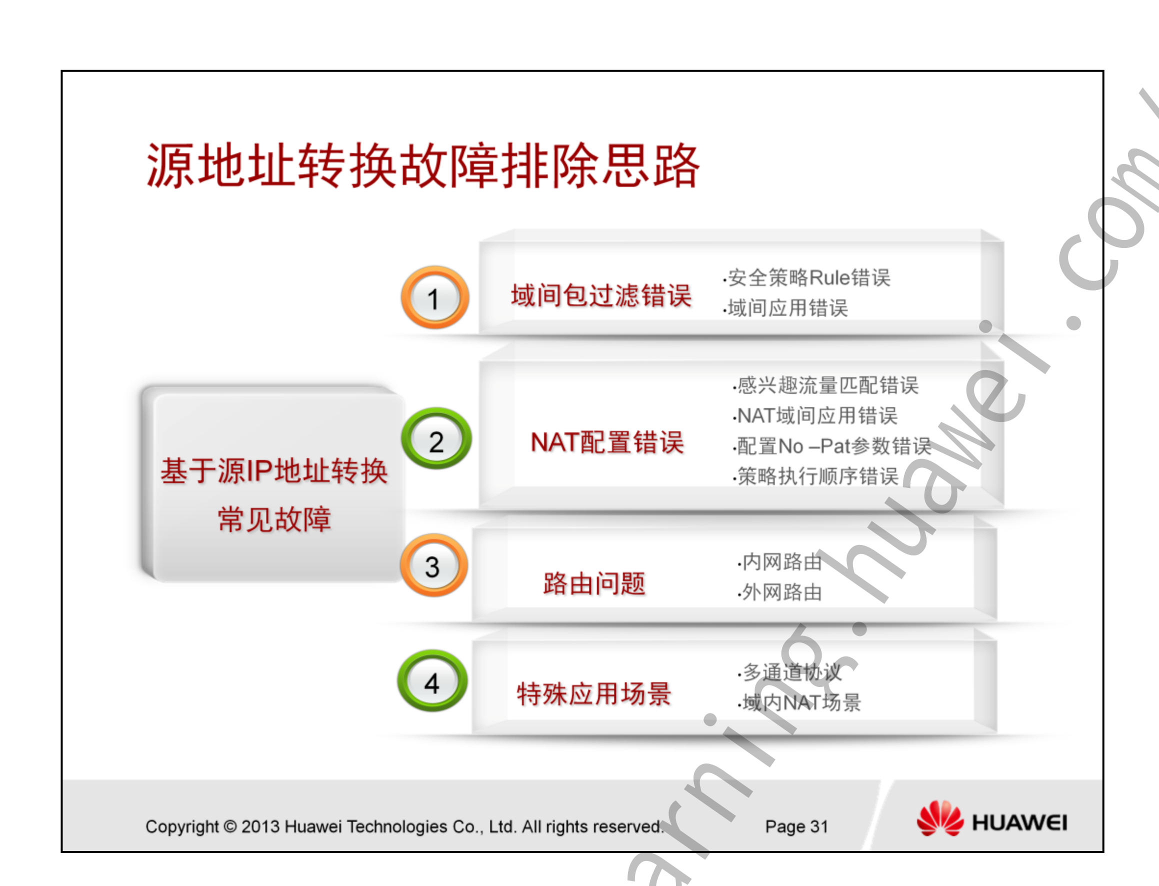
# 目录










源地址转换故障排除思路
基于源IP地址转换
常见故障
1
域间包过滤错误
·安全策略Rule错误
·域间应用错误
2
NAT配置错误
·感兴趣流量匹配错误
·NAT域间应用错误
·配置No –Pat参数错误
·策略执行顺序错误
3
路由问题
·内网路由
·外网路由
4
特殊应用场景
·多通道协议
·域内NAT场景
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 31
HUAWEI

## 源地址转换故障排除（一）

- 原因一：域间包过滤错误
- 原因二：NAT配置错误

```
nat-policy interzone trust untrust outbound
 policy 0
 action source-nat
 policy source 192.168.1.0 0.0.0.255
 address-group 1
```






原因一：域间包过滤错误

ACL配置错误（详情请参看包过滤故障排除）；

域间应用错误（详情请参看包过滤故障排除）。

原因二：NAT配置错误

感兴趣流量匹配错误：配置策略时，需要配置流量的source、destination及service-set，来定义需要进行NAT转换的流量。只有对策略中的感兴趣流量进行NAT转换，否则不进入NAT转换处理流程；

域间应用错误：策略要在合适的域间应用，并且域间的方向要选择正确，一般情况下，是由trust到untrust的outbound方向；

配置no-pat参数错误：配置no-pat参数后，会对内、外网地址进行一对一的转换，外网地址用完后，不会再对内网地址进行转换。这种情况，会造出部分内网终端间断行不能上网的现象；

策略执行顺序错误：配置多个策略时，默认执行顺序根据编号从小到大依次执行。可以通过policy move命令修改执行顺序。

## 源地址转换故障排除（二）

- 原因三：路由问题

```
<USG> display nat-policy interzone trust untrust inbound
nat-policy interzone trust untrust inbound
 firewall default packet-filter is permit
 nat-policy 0 (23424 times matched)
 action source-nat
 nat-policy source address-set a (group)
 address-group 1 no-pat
 nat-policy 5 (0times matched)
 action source-nat
 nat-policy source address-set b (group)
 address-group 2
```







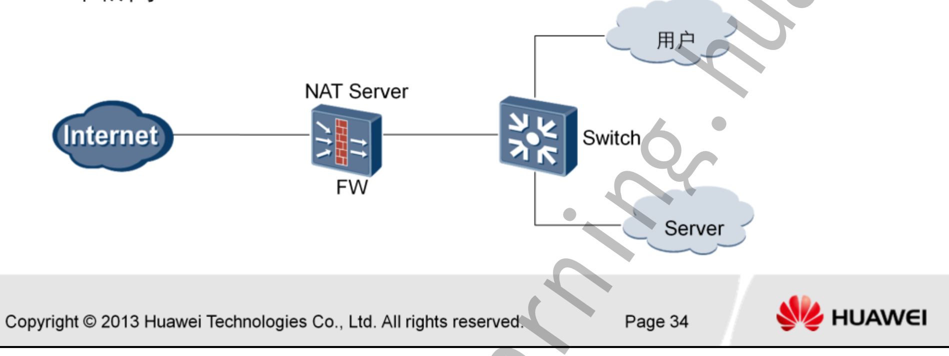

原因三：路由问题

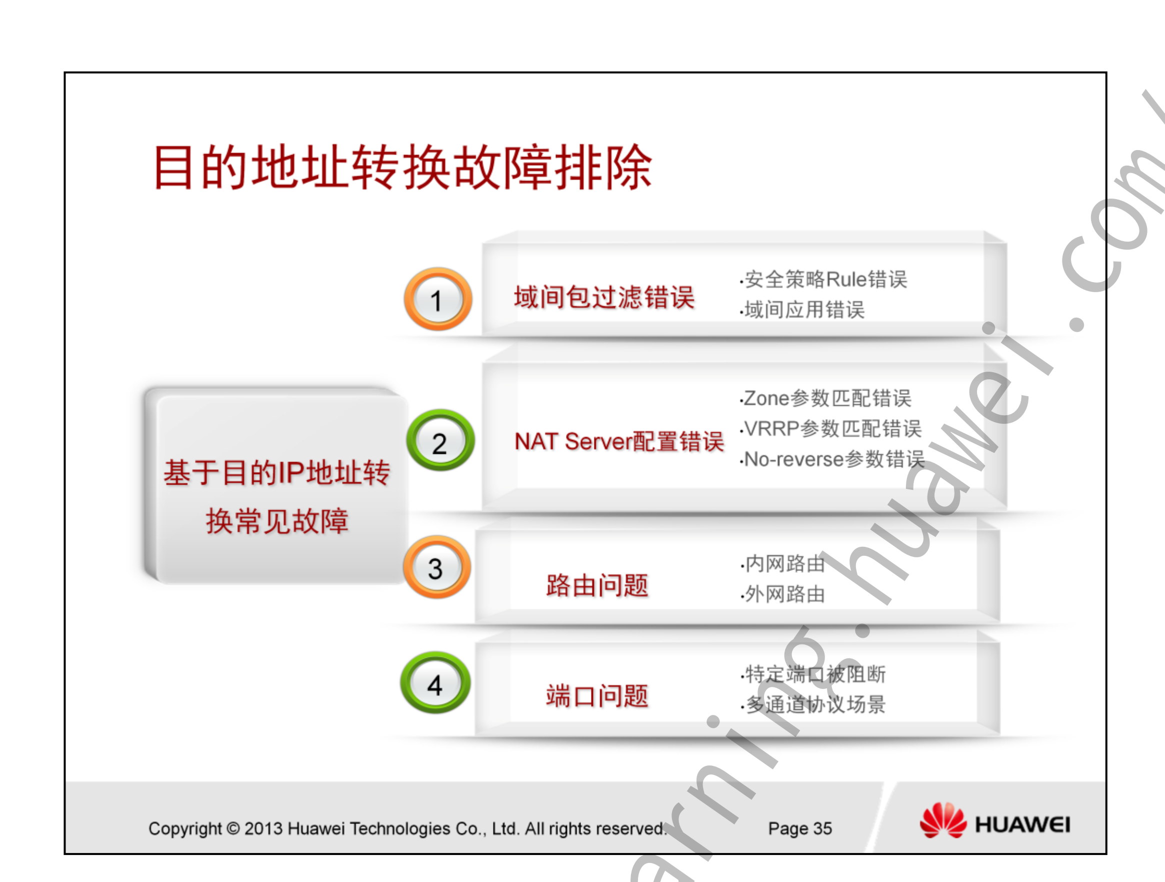
内网路由问题：终端不能上网，从防火墙上看没有该终端的会话，一方面的原因可能是因为包过滤的问题，另外也可能是该终端的报文没有到达防火墙，属于内网路由问题；

外网路由问题：运营商路由问题。

# 源地址转换故障排除（三）

- 原因四：特殊应用场景
  - **多通道协议**：如：FTP、MSN、PPTP、RSTP等，需要在域间开启NAT ALG功能，目的是识别多通道协议，并自动转换报文载荷中的IP地址和端口信息；
  - **域内NAT**：应用在域内，配置与域间NAT相同，主要应用场景如下图所示。




目的地址转换故障排除
基于目的IP地址转换常见故障
1
域间包过滤错误
·安全策略Rule错误
·域间应用错误
2
NAT Server配置错误
·Zone参数匹配错误
·VRRP参数匹配错误
·No-reverse参数错误
3
路由问题
·内网路由
·外网路由
4
端口问题
·特定端口被阻断
·多通道协议场景
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 35
HUAWEI

# 目的地址转换故障排除

- 原因一：域间包过滤错误
- 原因二：目的地址转换配置错误
- **原因三：路由问题**
- **原因四：端口问题**

```
<USG2200>dis cur | in nat server
nat server 0 global 1.1.1.1 inside 192.168.255.1 no-reverse
nat server 1 global 2.2.2.2 inside 10.0.0.1
<USG2200>dis firewall server-map
Nat Server, ANY -> 1.1.1.1[192.168.255.1], Zone: ---
  Protocol: ANY(Appro: ---), Left-Time: --:--:--, Addr-Pool: ---
  VPN: public -> public
Nat Server, ANY -> 2.2.2.2[10.0.0.1], Zone: ---
  Protocol: ANY(Appro: ---), Left-Time: --:--:--, Addr-Pool: ---
  VPN: public -> public
Nat Server Reverse, 10.0.0.1[2.2.2.2] -> ANY, Zone: ---
  Protocol: ANY(Appro: ---), Left-Time: --:--:--, Addr-Pool: ---
  VPN: public -> public
```




原因一：域间包过滤错误

ACL配置错误（详情请参看包过滤故障排除）；

域间应用错误（详情请参看包过滤故障排除）。

原因二：目的地址转换配置错误

zone参数配置错误：配置zone参数后，只对经过该安全域的流量进行地址转换。一般用在双出口或多出口的场景，访问流量要经过相关的安全域；

VRRP参数配置错误：global地址与VRRP虚地址在一个网段时，需要添加该参数。

no-reverce配置错误：添加该参数后，NAT Server不会添加反向静态server-map表项。访问内网服务器时回包匹配会话，而服务器不能主动访问外网，除非配置源地址转换。

原因三：路由问题

内网路由问题：如果可以查看有server-map正向回话的匹配，但没有反向匹配，需要查看到内网的路由问题；

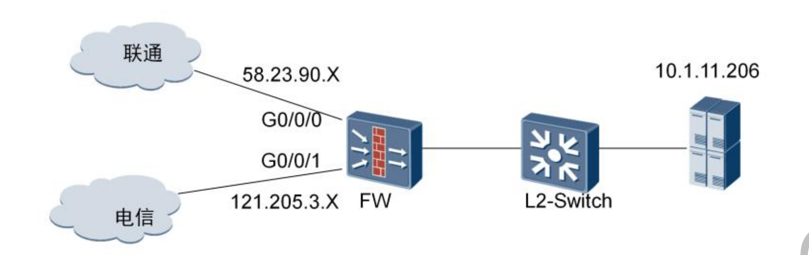
外网路由问题：运营商路由配置问题。

原因四：端口问题

特定端口被阻断：做端口的目的地址转换后，有时特定端口会被阻断，目前发现较多的情况有80、8080、8000端口；

多通道协议场景：查看是否配置NAT ALG。

# 案例：NAT Server双出口问题（一）




- **组网说明**
  - 121.205.3.X。联通地址58.23.90.X和电信地址121.205.3.X的8008端口分别映射到内部服务器8008端口。要求联通用户通过联通地址访问；电信用户通过电信地址访问。






# 案例：NAT Server双出口问题（二）

- 故障现象
  - nat server及路由配置如下：

    nat server 14 protocol tcp global 121.205.3.X 8008 inside 10.1.11.206 8008 no-reverse；

    nat server 15 protocol tcp global 58.23.90.X  8008 inside 10.1.11.206 8008 no-reverse；

    两条静态路由，路由优先级均为默认值60。
  - 通过电信公网地址可以访问内部服务器，但通过联通公网地址无法访问。





# 案例：NAT Server双出口问题（三）

- 处理过程
  - 排除包过滤、NAT Server等配置问题。
  - 去掉联通地址到内网地址的映射，ping联通地址可以通，且防火墙上可直接ping通服务器内网地址，排除路由问题。
  - 将联通映射端口改为10000到8008，telnet内容服务器的10000端口，不通，排除联通限制8008端口。
  - 联通访问内容服务器时，FW上查看会话，确认回包走电信链路；

```
tcp  VPN:public --> public
 Zone: untrust--> trust  TTL: 00:00:05  Left: 00:00:03
 Interface: Vlanif1  NextHop: 10.1.100.1  MAC: 80-fb-06-b0-0d-4d
 <--packets:0 bytes:0   -->packets:1 bytes:60
 218.17.167.151:2066-->58.23.90.58:8008[10.1.11.206:8008]

 tcp  VPN:public --> public
 Zone: trust--> untrust  TTL: 00:00:05  Left: 00:00:03
 Interface: GigabitEthernet0/0/0  NextHop: 121.205.3.1  MAC:
00-e0-fc-65-0c-01
 <--packets:0 bytes:0   -->packets:1 bytes:64
 10.1.11.206:8008[58.23.90.58:8008]-->218.17.167.151:2066
```






# 案例：NAT Server双出口问题（三）

- 原因分析
  - 联通用户发起请求，回复的报文走电信链路，运营商的链路上可能会存在链路状态检测的安全设备（并不是所有的运营商链路都会存在这种设备），这种设备会将来回路径不一致的报文丢弃，从而导致业务不通。
- 解决方法
  - FW上配置联通、电信网段的精确路由。这种解决方法配置的工作量太大，不易维护，而且如果联通用户通过访问电信的公网地址来访问内外业务，同样会出现来回路径不一致的问题；
  - 服务器上配置备用IP，联通、电信公网地址分别映射不同的服务器地址. 同时，FW上做策略路由，区分访问不同内网地址的流量，从相应的链路返回。







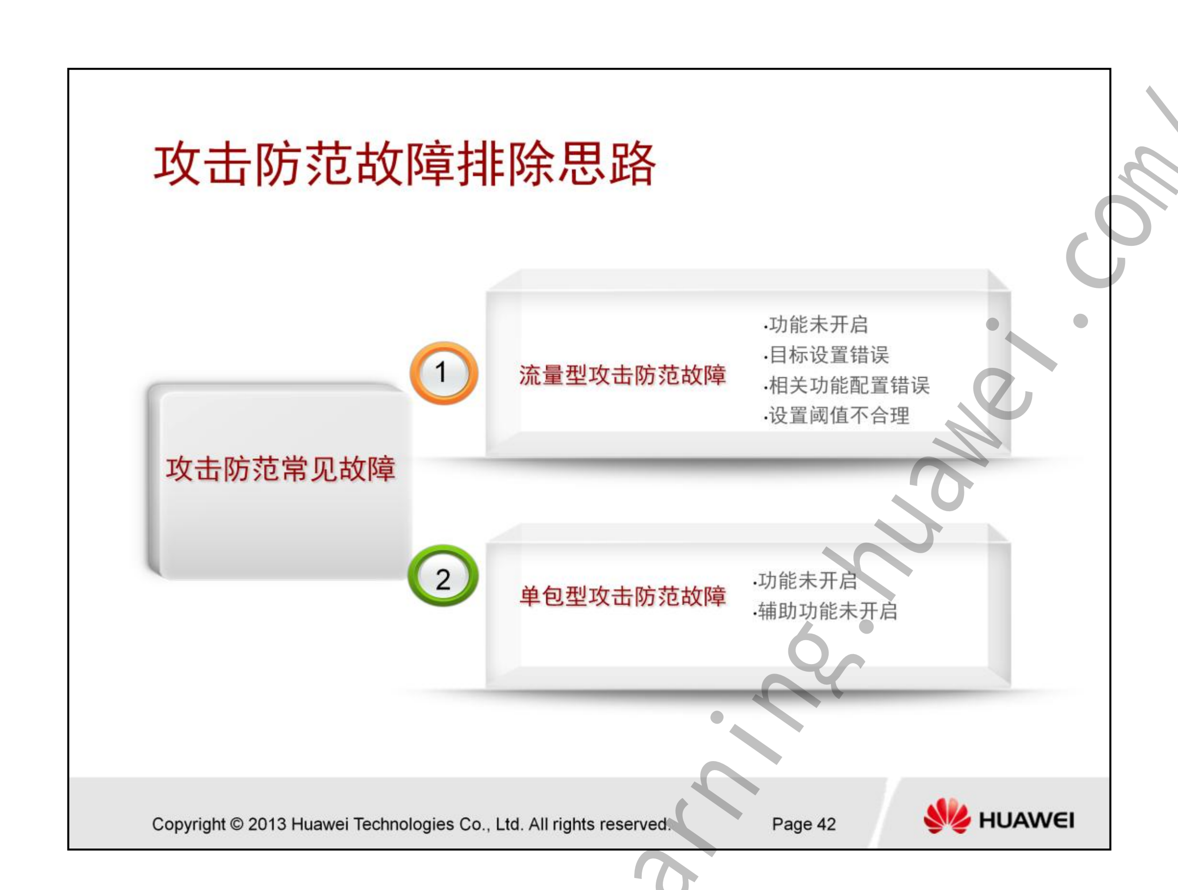
# 目录










攻击防范故障排除思路
攻击防范常见故障
1
流量型攻击防范故障
·功能未开启
·目标设置错误
·相关功能配置错误
·设置阈值不合理
2
单包型攻击防范故障
·功能未开启
·辅助功能未开启
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 42
HUAWEI

## 流量型攻击防范故障排除

- 基于**ICMP**、**UDP**的攻击防范
  - 基于**ICMP**的单包攻击：ping-of-death、large-icmp、icmp-redirect、tracert、icmp-unreachable、smurf
  - 基于**UDP**的单包攻击： fraggle
    - 排错步骤一：攻击防范开关是否开。
  - 基于**ICMP**的泛洪攻击：icmp-flood
  - 基于**UDP**的泛洪攻击：udp-flood
    - 排错步骤一：对应的攻击防范开关是否开启；
    - 排错步骤二：对应的需要保护的目的接口或者目的域是否配置正确,是否正确配置基于会话的速率限制；
    - 排错步骤三：设置的阈值是否合理。






基于接口的ICMP Flood攻击防范功能不能应用在交换口上。在物理接口和逻辑接口绑定的情况下，应将攻击防范应用在最高级别的逻辑接口上，攻击防范才能生效。例如：将物理接口ADSL接口和逻辑接口VE接口绑定，再将VE接口和Dialer接口绑定，则需将攻击防范应用在Dialer接口，攻击防范才能生效。

基于安全区域的ICMP Flood攻击防范功能按该安全区域发送的ICMP报文总量来判断是否超出阈值。配置基于会话的ICMP速率限制,可以针对每条会话设定一个ICMP报文速率阈值。当USG发现会话的报文速度超过设定的阈值时，则认为发生攻击，锁定此会话，后续此会话的报文不再允许报文通过。当此会话连续3秒或者3秒以上没有流量时，解锁此会话，后续此会话的报文可以继续通过。

## 攻击防范故障排除思路

- 基于TCP的攻击防范
  - 基于TCP的单包攻击：land、winnuke、tcp-flag
    - 排错步骤一：攻击防范开关是否开启
  - 基于TCP的泛洪攻击：syn-flood
    - 排错步骤一：对应的攻击防范开关是否开启
    - 排错步骤二：是否开启反向源探测、TCP代理功能
    - 排错步骤三：是否配置包或会话的间隔时间，时间配置是否合理
- 基于IP的攻击防范
  - 基于IP的选项攻击：route-record、source-route、time-stamp
    - 排错步骤一：攻击防范开关是否开启
  - 基于IP的路由攻击：ip-spoofing
    - 排错步骤一：对应的攻击防范开关是否开启






基于接口的SYN Flood攻击防范功能不能应用在交换口上。在物理接口和逻辑接口绑定的情况下，应将攻击防范应用在最高级别的逻辑接口上，攻击防范才能生效。例如：将物理接口ADSL接口和逻辑接口VE接口绑定，再将VE接口和Dialer接口绑定，则需将攻击防范应用在Dialer接口，攻击防范才能生效。

基于安全区域的SYN Flood攻击防范功能按该安全区域发送的SYN报文总量来判断是否超出阈值。

## 攻击防范故障排除思路

- 基于扫描的攻击防范
  - 基于IP扫描的攻击：ip-sweep
    - 排错步骤一：攻击防范开关是否开启
    - 排错步骤二：黑名单功能是否开启
    - 排错步骤三：地址扫描速率是否合理设置
  - 基于端口扫描的攻击：port-scan
    - 排错步骤一：攻击防范开关是否开启
    - 排错步骤二：黑名单功能是否开启
    - 排错步骤三：端口扫描速率是否合理设置
- 基于分片的攻击防范
  - 基于分片的攻击： ip-fragment、teardrop
    - 排错步骤：攻击防范开关是否开启








配置IP地址扫描攻击防范参数后，设备对进入的TCP，UDP，ICMP报文进行检测，并以某个源IP地址为索引，判断该源IP地址发送报文的目的IP与前一报文的目的IP地址是否不同，如果是则异常次数加1。当异常频率超过预定义的阈值时，则认为该源IP地址的报文为IP地址扫描攻击，并将该源IP地址加入黑名单，然后做如下处理：

若USG开启黑名单功能，则从该源IP地址发出的报文命中黑名单被全部丢弃；

若USG没有开启黑名单功能，则从该源发出的报文，如果扫描速率超过了设定的阈值，超出部分则丢弃，其余部分进行转发。

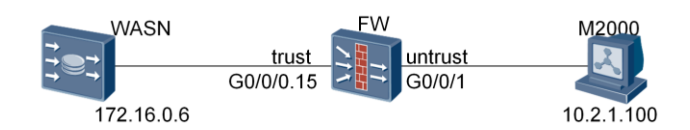
IP报文头中的DF和MF标志位用于分片控制，攻击者通过发送分片控制非法的报文，从而导致主机接收报文时产生故障，报文处理异常，甚至导致主机崩溃。开启IP分片报文攻击防范功能，设备将检测到报文控制位是下列情况之一时，则直接丢弃并记录攻击日志：

DF位为1，而MF位也为1；

DF位为1，而Offset > 0；

DF位为0，而分片 Offset + Length > 65535。

# 案例：攻击防范导致业务不通（一）




- 故障现象
  - FW作为安全设备接入M2000和WASN之间，开启攻击防范，保护WASN；M2000与WASN通过TCP建立连接，进行数据交互。目前的现象是，TCP连接可以建立，但数据交互不成功。





# 案例：攻击防范导致业务不通（二）

- 原因分析

```
tcp  VPN: public -> public
Zone: untrust -> trust  Tag: 0x2588  State: 0x53
TTL: 00:20:00  Left: 00:19:19  Id: 17244a80  SlvId: 2efdff40
Interface: G0/0/0.15  Nexthop: 172.26.0.6  MAC: 00-25-9e-f1-db-35
<-- packets:24 bytes:1131   --> packets:24 bytes:4181
172.26.0.6:6000<--10.2.1.100:38287

tcp  VPN: public -> public
Zone: untrust -> trust  Tag: 0x2588  State: 0x53
TTL: 00:20:00  Left: 00:19:58  Id: 2c9a3ce0  SlvId: 113ba800
Interface: G0/0/0.15  Nexthop: 172.26.0.6  MAC: 00-25-9e-f1-db-35
<-- packets:148 bytes:16182   --> packets:216 bytes:55200
172.26.0.6:16002<--10.2.1.100:38285
```

```
tcp  VPN: public -> public
Zone: untrust -> trust  Tag: 0x2588  State: 0x56
TTL: 00:00:10  Left: 00:00:05  Id: 17244a80  SlvId: 2efdff40
Interface: G0/0/0.15  Nexthop: 172.26.0.6  MAC: 00-25-9e-f1-db-35
<-- packets:26 bytes:1211   --> packets:26 bytes:4261
172.26.0.6:6000<--10.2.1.100:38287

tcp  VPN: public -> public
Zone: untrust -> trust  Tag: 0x2588  State: 0x56
TTL: 00:00:10  Left: 00:00:05  Id: 2c9a3ce0  SlvId: 113ba800
Interface: G0/0/0.15  Nexthop: 172.26.0.6  MAC: 00-25-9e-f1-db-35
<-- packets:163 bytes:17674   --> packets:236 bytes:60447
172.26.0.6:16002<--10.2.1.100:38285
```

```
58 2010-09-29 18:17:06.227208 10.2.1.100   172.26.0.6   TCP   [TCP segment of a reassembled PDU]
76 2010-09-29 18:17:10.645293 10.2.1.100   172.26.0.6   TCP   [TCP Retransmission] [TCP segment of a reassembled PDU]
87 2010-09-29 18:17:16.483712 10.2.1.100   172.26.0.6   TCP   [TCP Retransmission] [TCP segment of a reassembled PDU]
113 2010-09-29 18:17:30.140859 10.2.1.100  172.26.0.6   TCP   [TCP Retransmission] [TCP segment of a reassembled PDU]
156 2010-09-29 18:17:57.433182 10.2.1.100  172.26.0.6   TCP   [TCP Retransmission] [TCP segment of a reassembled PDU]
267 2010-09-29 18:18:51.998814 10.2.1.100  172.26.0.6   TCP   [TCP Retransmission] [TCP segment of a reassembled PDU]
382 2010-09-29 18:19:51.625589 10.2.1.100  172.26.0.6   TCP   [TCP Retransmission] [TCP segment of a reassembled PDU]
611 2010-09-29 18:20:06.084282 10.2.1.100  172.26.0.6   TCP   [TCP segment of a reassembled PDU]
633 2010-09-29 18:20:50.251445 10.2.1.100  172.26.0.6   TCP   [TCP Retransmission] [TCP segment of a reassembled PDU]
```







原因分析

查看TCP连接建立正常；

抓包查看后续的数据传输出现问题，TCP不断重传；

观察FW会话TCP连接建立后，过20秒钟会话变为半连接，期间无数据传输。

# 案例：攻击防范导致业务不通（三）

- 原因分析

| | | | | | | |
|---|---|---|---|---|---|---|
| 692 | 2010-09-29 | 23:10:06.450243 | 10.2.1.100 | 172.26.0.6 | TCP | 60943 > 6001 [SYN] Seq=0 Len=0 MSS=1460 WS=0 |
| 693 | 2010-09-29 | 23:10:06.451322 | 172.26.0.6 | 10.2.1.100 | TCP | 6001 > 60943 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=512 |
| 694 | 2010-09-29 | 23:10:06.451547 | 10.2.1.100 | 172.26.0.6 | TCP | 60943 > 6001 [ACK] Seq=1 Ack=1 Win=49664 Len=0 |
| 695 | 2010-09-29 | 23:11:07.064325 | 10.2.1.100 | 172.26.0.6 | TCP | [TCP segment of a reassembled PDU] |
| 696 | 2010-09-29 | 23:11:07.182467 | 172.26.0.6 | 10.2.1.100 | TCP | 6001 > 60943 [ACK] Seq=1 Ack=11 Win=8184 Len=0 |
| 697 | 2010-09-29 | 23:11:08.564682 | 172.26.0.6 | 10.2.1.100 | X11 | Event: <Unknown eventcode 43>, <Unknown eventcode 48>, Colorm |
| 698 | 2010-09-29 | 23:11:09.332177 | 172.26.0.6 | 10.2.1.100 | X11 | [TCP Retransmission] Event: <Unknown eventcode 43>, <Unknown |
| 699 | 2010-09-29 | 23:11:09.332185 | 10.2.1.100 | 172.26.0.6 | TCP | 60943 > 6001 [ACK] Seq=11 Ack=163 Win=49664 Len=0 |
| 700 | 2010-09-29 | 23:12:06.669568 | 10.2.1.100 | 172.26.0.6 | TCP | [TCP segment of a reassembled PDU] |
| 701 | 2010-09-29 | 23:12:06.786973 | 172.26.0.6 | 10.2.1.100 | TCP | 6001 > 60943 [ACK] Seq=163 Ack=21 Win=8184 Len=0 |
| 702 | 2010-09-29 | 23:12:07.140646 | 172.26.0.6 | 10.2.1.100 | TCP | [TCP segment of a reassembled PDU] |
| 703 | 2010-09-29 | 23:12:07.258055 | 10.2.1.100 | 172.26.0.6 | TCP | 60943 > 6001 [ACK] Seq=21 Ack=283 Win=49664 Len=0 |
| 704 | 2010-09-29 | 23:12:07.259955 | 172.26.0.6 | 10.2.1.100 | X11 | Event: <Unknown eventcode 101> |
| 705 | 2010-09-29 | 23:12:07.379679 | 10.2.1.100 | 172.26.0.6 | TCP | 60943 > 6001 [ACK] Seq=21 Ack=325 Win=49664 Len=0 |
| 706 | 2010-09-29 | 23:13:06.284314 | 10.2.1.100 | 172.26.0.6 | TCP | [TCP segment of a reassembled PDU] |
| 707 | 2010-09-29 | 23:13:06.414192 | 172.26.0.6 | 10.2.1.100 | TCP | 6001 > 60943 [ACK] Seq=325 Ack=31 Win=8185 Len=0 |

- 解决方法
  - 客户的业务和应用场景与攻击防范的tcp-illeage-session防护类型相冲突，最直接的方法就是取消tcp-illeage-session防护。另外，如果可行，也可以与客户沟通更改应用协议的某些参数，来规避这种冲突。








绕过FW，业务访问正常，抓包分析：M2000与WASN建立TCP连接，等待1分钟后才会有数据的交互。FW上开启tcp-illeage-session攻击防范,TCP连接建立后，如果15秒内无数据相应数据报文，则认为该TCP连接为攻击，断开连接，从而导致业务中断。



# 目录









# 限流策略排除思路

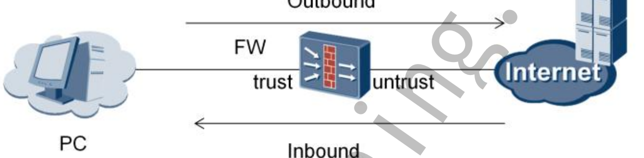
- 配置整体限流策略功能
  - 检查是否启用限流功能
  - 检查整体限流Class
  - 检查整体限流策略
- 配置每IP限流策略功能
  - 检查是否启用限流功能
  - 检查每IP限流Class
  - 检查每IP限流策略
  - 整体限流Class
  - 检查整体限流策略





# 限流策略故障排除

- **故障点1：未启用限流策略功能**
  - 执行命令traffic-policy enable，启用限流策略功能。
- **故障点2：限流策略优先级顺序和方向设置错误**
  - 每个域间的Inbound和Outbound方向上可以应用多个限流策略。
  - Inbound：入方向，低安全级别的安全区域向高安全级别的安全区域的方向。
  - Outbound：出方向，高安全级别的安全区域向低安全级别的安全区域的方向。



## 限流策略故障排除

- **故障点3：包括最大带宽、保证带宽、最大连接数数值设置错误**
  - 必须保证每IP的保证带宽的总值要小于整体带宽的值。
  - 如果还需要限制每个IP的最大带宽还可以配置每IP最大带宽。所有IP的最大带宽的和要大于整体带宽，否则保证带宽无意义。
  - 整体限流策略和每IP限流策略控制的IP范围需一致。








故障点3：包括最大带宽、保证带宽、最大连接数数值设置错误

必须保证每IP的保证带宽的总值要小于整体带宽的值，这个需要先根据网络规划计算保证，保证带宽的总和不超过接口的总带宽，如果所有的流量加起来超过了运营商给的带宽，就会在接口处随机丢包了。

一般情况下配置保证带宽的时候只配置每IP保证带宽、整体带宽就行了，如果还需要限制每个IP的最大带宽还可以配置每IP最大带宽。此时所有IP的最大带宽的和要大于整体带宽，否则保证带宽无意义。例如：某网段有10个IP，配置的整体带宽为50M，则其保证带宽可以配置为4M左右（小于5M），最大带宽可配置为10M左右（大于5M），这时可以满足保证带宽的场景需求。

整体限流策略和每IP限流策略控制的IP范围需一致，因为如果二者不一致，当整体带宽较小时，没有配置保证带宽的IP会因为无法抢占配置了保证带宽的IP的流量，而导致允许通过流量的很少。



# 目录

1. 故障排除方法
2. 安全策略故障排除
3. 防火墙高级安全特性故障排除
4. 双机热备故障排除
5. L2TP VPN故障排除
6. IPSEC VPN故障排除
7. SSL VPN故障排除








双机热备故障排错思路
双机热备常见故障
1
组网问题
·硬件要求
·软件要求
2
配置错误
·VRRP VGMP配置问题
·HRP配置错误
3
主备切换问题
·路由可达问题
·端口检测问题
4
结合使用问题
·与NAT结合使用问题
·与OSPF结合使用问题
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 54
HUAWEI

## 双机热备故障排错思路（一）

- 故障点一：设计问题
  - **硬件要求**：要求进行双机热备份的两台设备接口卡的位置、类型和数目都相同，且需要加入到相同的安全域，否则会出现主用USG备份过去的信息，与备用USG的物理配置无法兼容，导致主备USG切换后出现问题；
  - **软件要求**：软件版本和BootRoom版本一致。
- 故障点二：配置问题
  - **VRRP/VGMP配置类问题**：请参考备注或手册；
  - **HRP配置问题**：请参考备注或手册。



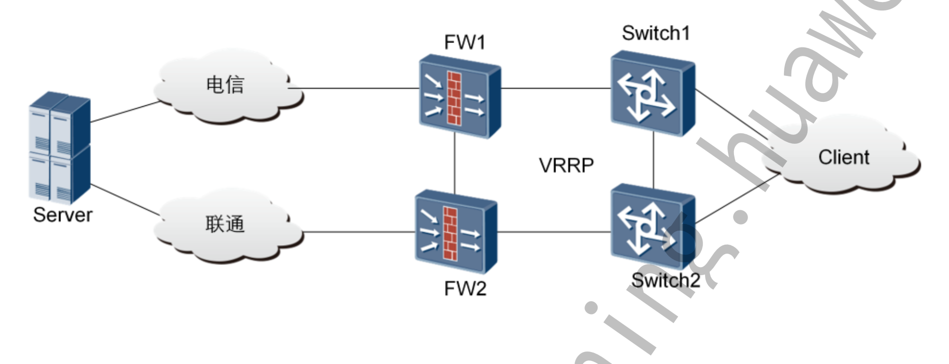



由于VGMP报文不支持分片，请不要在接口上配置MTU。否则，将可能导致USG不能正常接收VGMP报文。当主用USG出现故障时，主备USG不能正常切换。USG支持VRRP备份组的虚拟IP地址与对应的接口IP地址在同一网段和不在同一网段两种情况。

主备USG的HRP备份通道配置必须一致。主备USG的HRP备份通道接口必须直接相连，中间不能连接交换机。HRP备份通道接口不能为二层交换接口或VlanIf接口。 USG支持使用Eth-Trunk接口做为HRP备份通道，既提高了可靠性，又增加了备份通道的带宽。

# 双机热备故障排错思路（二）

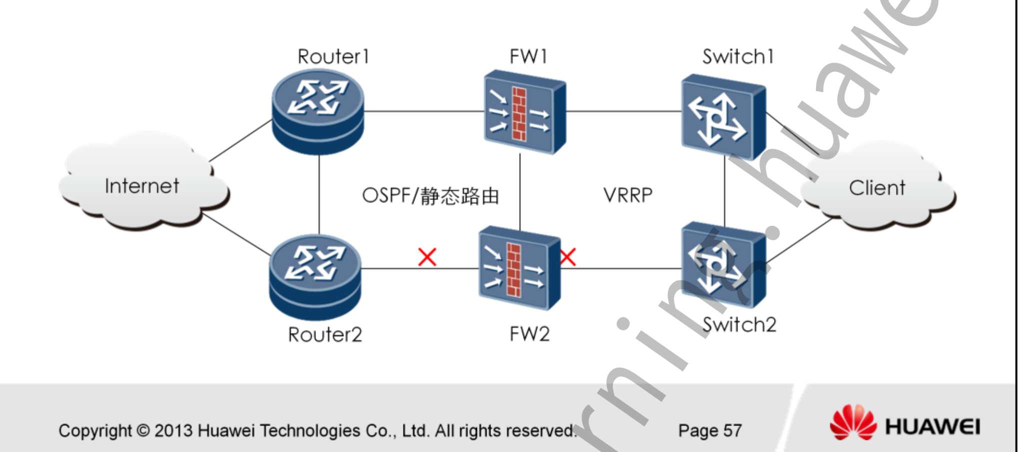
- 故障点三：主备切换问题
  - 路由可达性问题：业务在双链路上运行，需要配置IP-Link，并与HRP绑定，实现二层或三层链路的可达性监控。目的路由不可达时，HRP触发VGMP组切换。





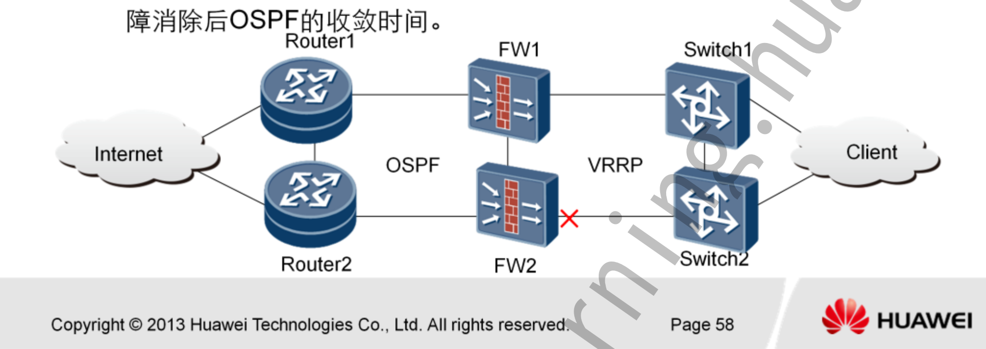

# 双机热备故障排错思路（三）

- 本地链路监控问题：同一台设备上，部分端口运行VRRP，部分不运行，需要通过在运行VRRP的端口上监控未运行VRRP的端口（Link-Group），以实现正常切换。



# 双机热备故障排错思路（四）

- 故障点四：双机热备与NAT结合使用场景
  - 虚拟IP与地址池在一个网段时，需要将NAT与VRRP组相关联；不在一个网段时，则不需要关联。
- 故障点五：双机热备与OSPF结合使用场景
  - 防火墙一侧运行VRRP，另一侧运行OSPF，需要通过命令hrp ospf-cost adjust-enable，配置根据HRP状态调整OSPF相关的COST值命令功能。
  - 如果配置了VGMP组的主动抢占功能，则需要配置抢占延迟时间大于故障消除后OSPF的收敛时间。

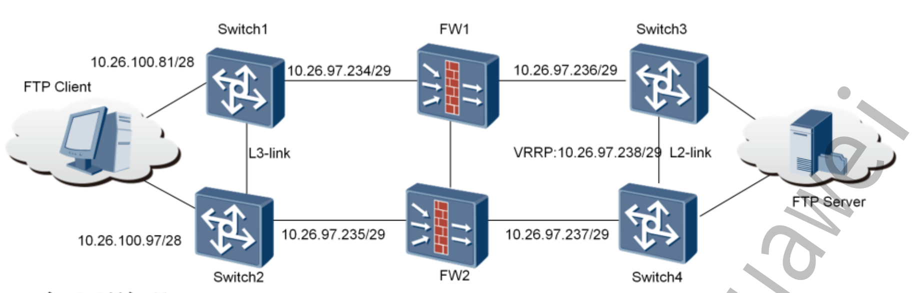





HUAWEI

配置hrp ospf-cost adjust-enable后，当链路发生故障，缺省情况下，OSPF COST值调整为为65500。

# 案例:来回路径不一致导致FTP业务不通






- 组网说明
  - 防火墙FW1、FW2以透明模式接入到网络;
  - Switch1、Switch2运行双机热备，心跳报文通过Switch3、Switch4交互;Switch3、Switch4也运行双机热备，心跳报文通过直连二层链路交互。
- 故障现象
  - FTP Client能ping通FTP Server （第一个ping包不通） ，但FTP业务不通。

## 案例:来回路径不一致导致FTP业务不通

- 处理过程

```
<gprsadm@GGSNWH08_RE0> traceroute 10.25.5.71
traceroute to 10.25.5.71 (10.25.5.71), 30 hops max, 40 byte packets
 1  10.26.100.97 (10.26.100.97)  0.379 ms  0.310 ms  0.348 ms
 2  10.26.97.236 (10.26.97.236)  2.411 ms  2.350 ms  2.524 ms
 3  10.25.253.1 (10.25.253.1)  0.529 ms  0.556 ms  0.463 ms
```

- 原因分析
  - Ping测试第一个报文丢弃；
  - FTP业务不通原因。
- 解决方法
  - 通过命令hrp mirror session enable；
  - 通过命令undo firewall session link-state check。







- 处理过程

可以ping通FTP Server，排除路由问题；

通过检查，域间包过滤及ASPF均配置正确；

通过tracert测试，确认来回路径不一致。

- 原因分析

Ping测试第一个报文丢弃，原因有两种可能：

发送ping前，源需要请求目的的MAC地址，即发送ARP请求，如果ARP应答报文返回时间过长，超过ping request time out 时间，将认为系统不通；

来回路径不一致，假设ping的请求报文通过主防火墙FW1，返回的应答报文经过FW2，那么可能会造成第一个ping包的丢包。原因为：双机热备会话表的备份时间要比防火墙创建会话表的时间晚几秒钟，而这个时间恰好超过了系统的ping request  time out 时间，所以第一个ping报文会被丢弃。

FTP业务不通原因：FTP的控制通道的建立是基于TCP的，客户端通过syn-request报文发起TCP连接，服务器回复syn-ack响应，由于syn-ack报文通过FW2防火墙，而防火墙上无相应会话，所以防火墙会丢弃该报文，导致FTP的控制通道无法建立，因此业务不通。

- 解决方法

通过命令hrp mirror session enable，打开防火墙快速备份功能，保证会话备份没有延迟，备份口要使用主控板上的口；

通过命令undo firewall session link-state check，关闭链路状态检测，打开双向的包过滤。



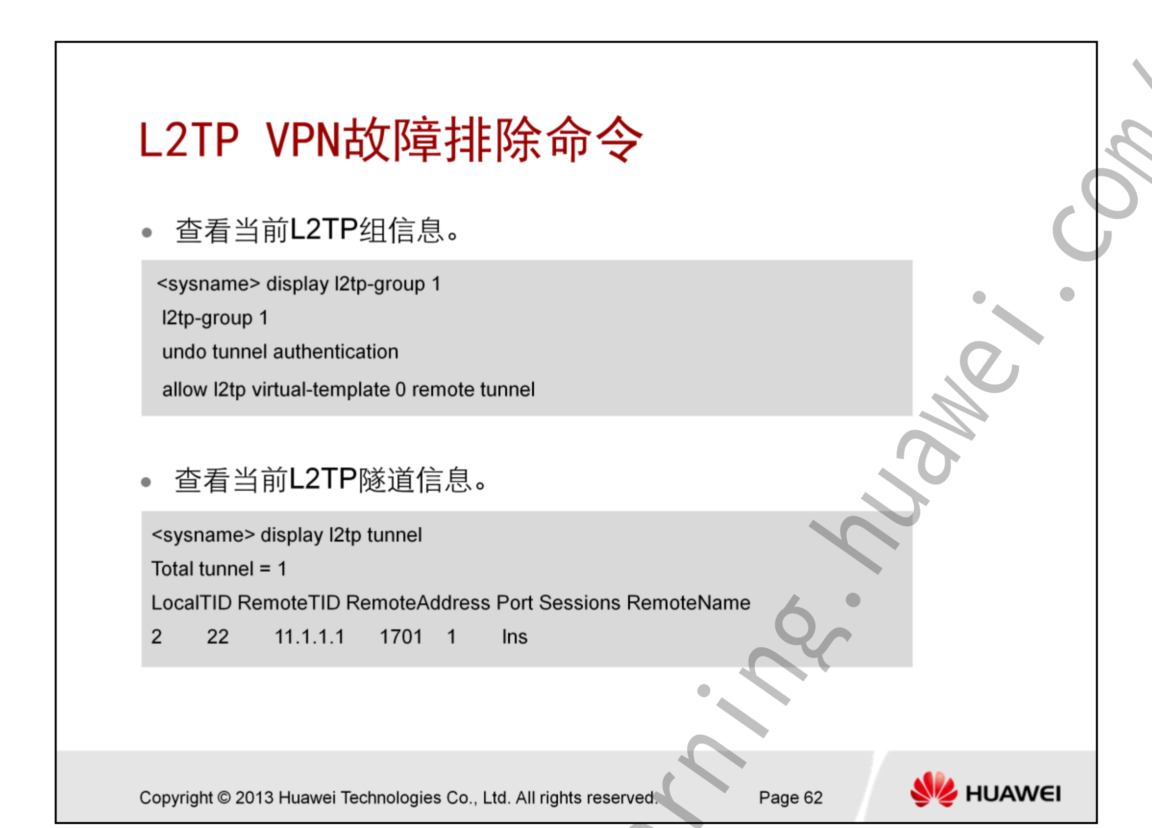
# 目录





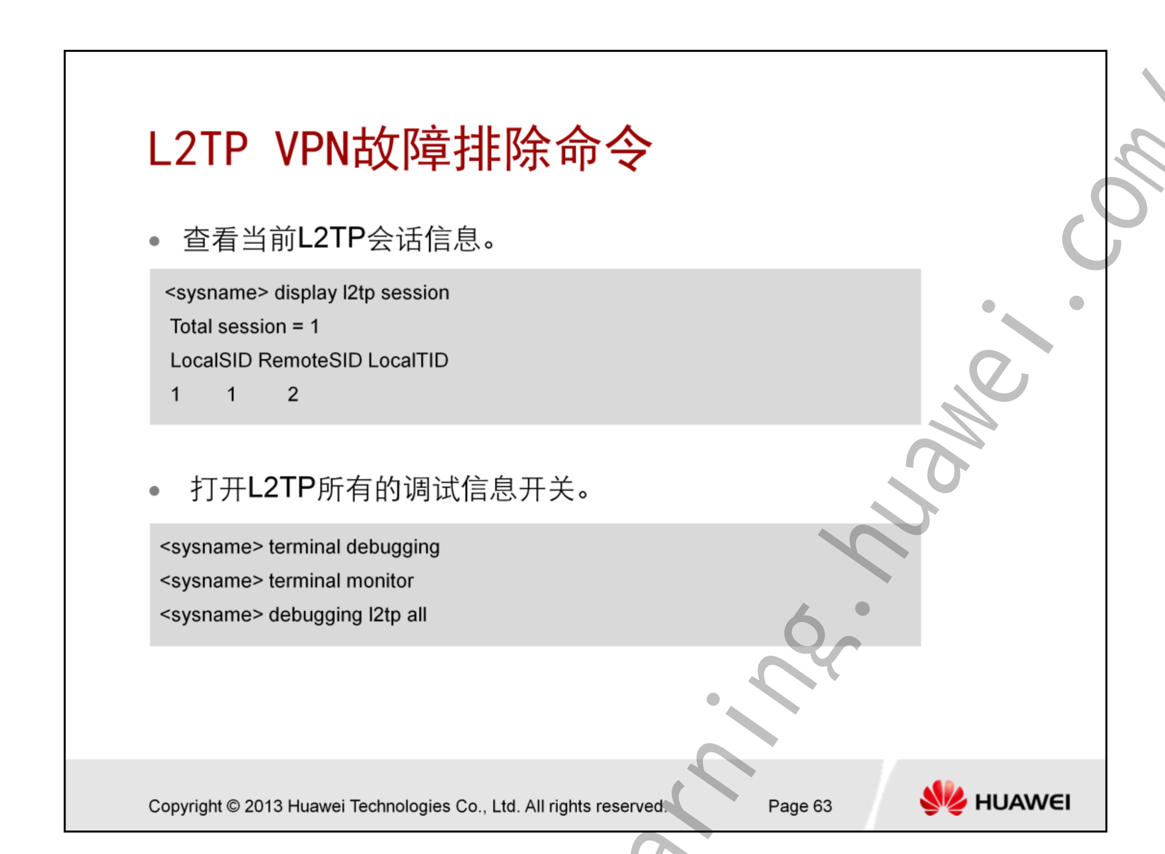







display l2tp tunnel命令查看l2tp是否拨号成功；

查看设备会话信息，也是排错中非常实用的命令，即display firewall session table，可以查看是否存在l2tp vpn的会话。




当通过配置无法排查l2tp故障原因时，使用debug信息来调式出l2tp交互的打印信息，有助于我们分析故障原因。在输出完debug信息之后，请及时关闭debug开关（undo debugging all）。

# Debug命令使用举例

- 在LAC打开debug ppp all若看到如下信息时则为认证未通过，需要检查用户名密码是否与aaa配置一致。 PAP认证没通过信息如下：

```
*0.7832210 E200E-B PPP/7/debug2:
  PPP Error:
     Virtual-Template1:0 PAP : Server failed No.  1 !
```

- CHAP认证没有通过信息如下：

```
PPP Packet:
    Virtual-Template1:0 Output CHAP(c223) Pkt, Len 33
    State ServerFailed, code FAILURE(04), id 1, len 29
    Message: Illegal User or password.

*0.12783270 E200E-B PPP/7/debug2:
 PPP Error:
    Virtual-Template1:0 CHAP : Server auth failed No.  1 !
 *0.12783410 E200E-B PPP/7/debug2:
```






debug信息中NO.1表示第几次认证失败，1表示第一次，最多是3次。

## Debug命令使用举例

- LAC向LNS发起了l2tp的协商但是LNS没有回应
  - 打开lns端l2tp的debug，如果有下面显示信息，说明lns端remote name 与lac端配置tunnel name不一致。通常lac端发起协商，而lns未回应则需检查l2tp隧道两端参数是否一致。

```
*0.15558990 E200E-B L2TP/7/L2TDBG: L2TP::requested host isn't in the define
   l2tp  group , refuse the requested
```







如果LNS使用的是radius认证，而radius认证配置不正确，此时也会导致LNS不会回应LAC。



# 目录

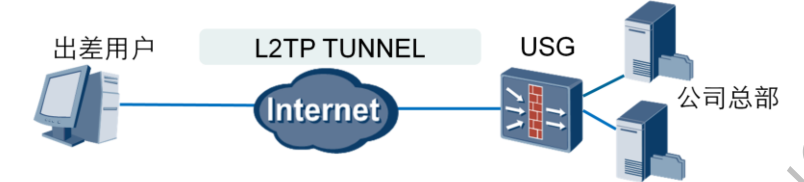








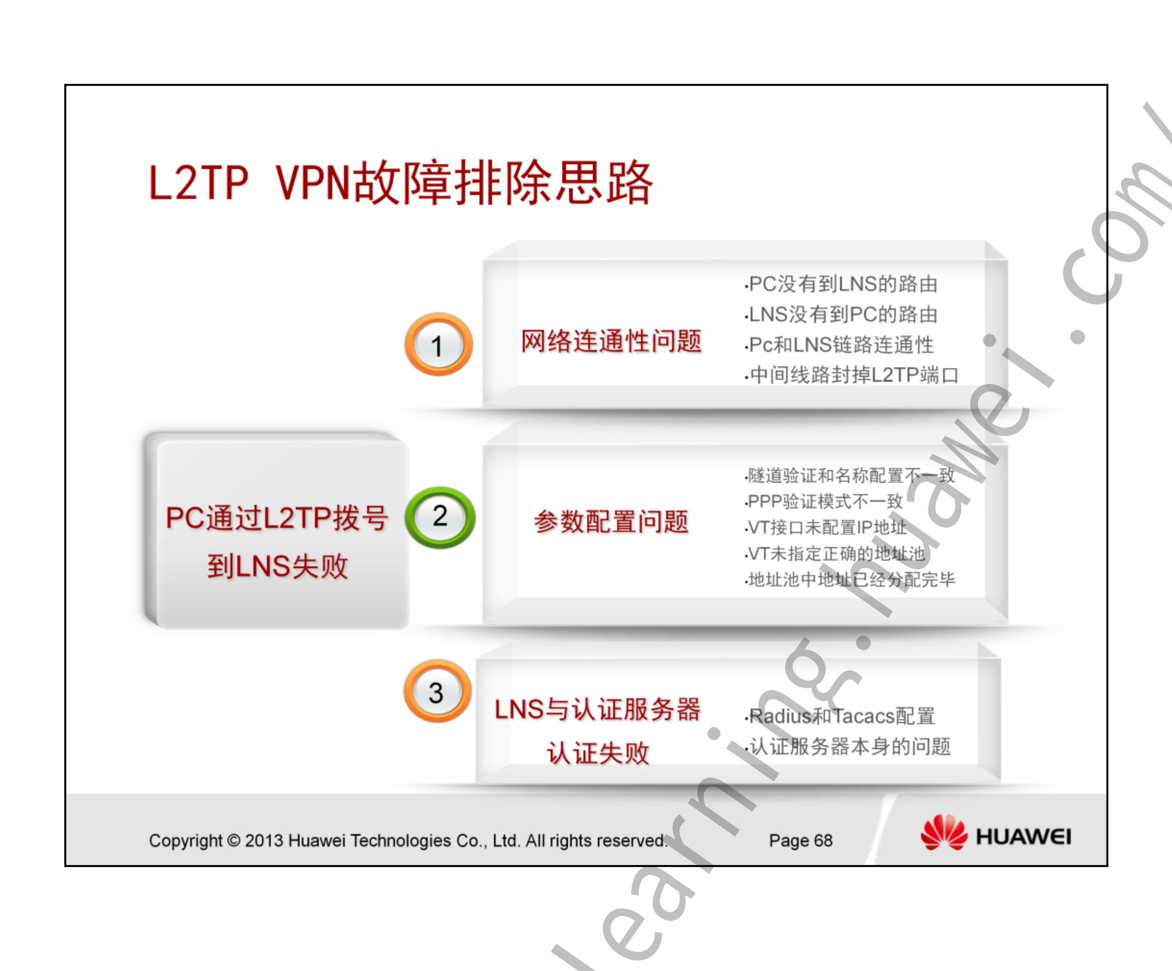
# 故障排除：Client-Initialized方式




- 现象描述
  - 出差员工或者分支机构员工通过L2TP访问公司总部资源；
  - 总部对外出口网关，在使用PC进行拨号时，拨号失败。
- 可能原因
  - 原因一：网络连通性问题；
  - 原因二：参数配置问题；
  - 原因三：LNS与认证服务器联动不成功。







L2TP VPN故障排除思路
PC通过L2TP拨号到LNS失败
1
网络连通性问题
·PC没有到LNS的路由
·LNS没有到PC的路由
·Pc和LNS链路连通性
·中间线路封掉L2TP端口
2
参数配置问题
·隧道验证和名称配置不一致
·PPP验证模式不一致
·VT接口未配置IP地址
·VT未指定正确的地址池
·地址池中地址已经分配完毕
3
LNS与认证服务器认证失败
·Radius和Tacacs配置
·认证服务器本身的问题
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 68
HUAWEI

# L2TP VPN故障排除步骤

- 原因一：网络连通性问题
  - PC没有到LNS的路由

    在PC上查看路由命令：route print
  - LNS没有到PC的路由

    防火墙上查看路由命令：display ip routing-table
  - PC和LNS之间的链路存在连通性故障

    比如：中间线路的接口，线缆故障，设备路由等等因素。
  - 中间链路封掉了l2tp端口

    如果其他端口业务都正常，但是LNS设备无法接收到l2tp数据报文，那么中间链 路的设备禁止了l2tp端口。






判定是否是中间链路问题，可以使用ping或者tracert命令。

## L2TP VPN故障排除步骤

- 原因二：参数配置问题
  - 隧道验证配置不一致

    查看LNS是否启用隧道验证，如果启用隧道验证，将会显示隧道验证方式和隧道验证使用的密码。

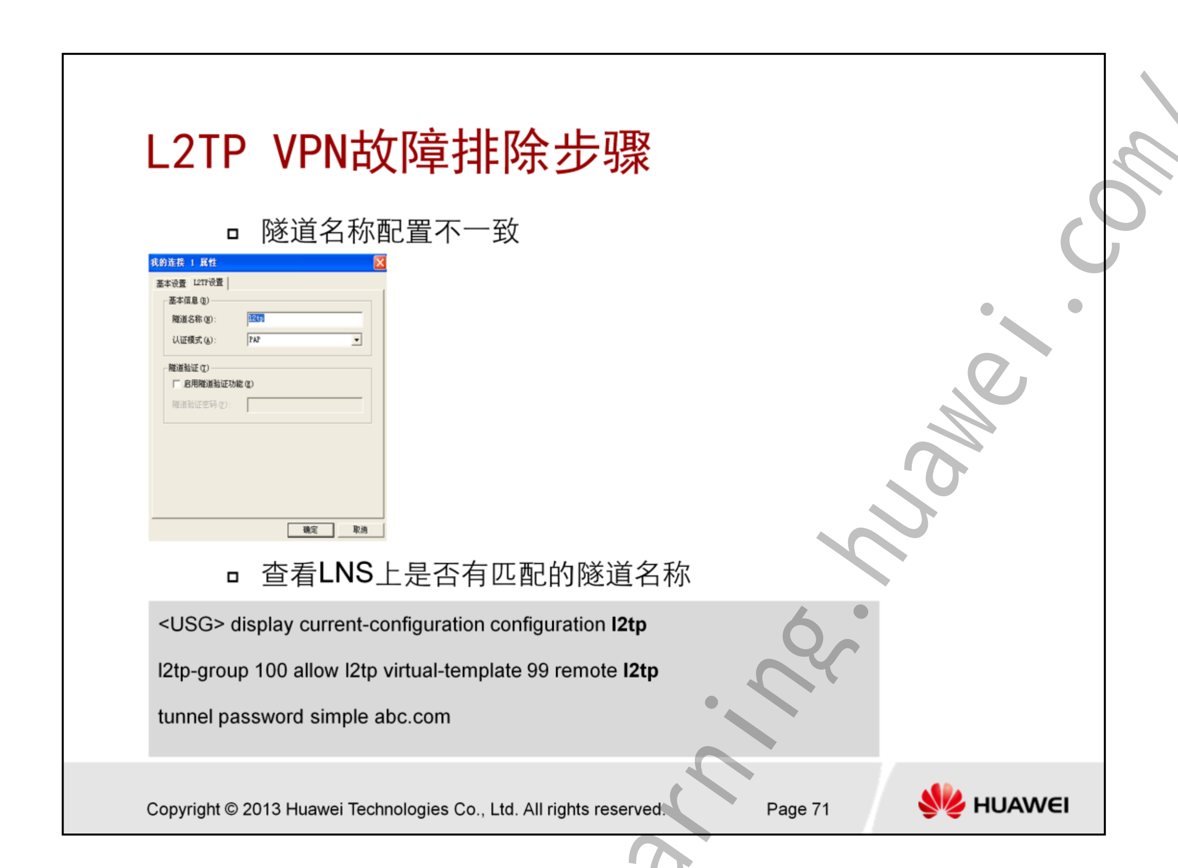
```
<USG> display current-configuration configuration l2tp
 l2tp-group 100
allow l2tp virtual-template 99 remote l2tp
tunnel password simple abc.com
```

检查LNS和拨号客户端是否都同时启用隧道验证。检查拨号客户端配置的隧道验证密码是否与LNS上配置的隧道验证密码相同。






默认情况下隧道验证是开启的，因此需要配置隧道密码。如果不使用隧道验证，在l2tp-group视图下：undo tunnel authentication。




如果在LNS上配置了remote名字，在客户端上的隧道名称必须和该remote名字一致。如果使用l2tp-group 1，那么LNS允许所有客户端拨入；如果使用其他l2tp-group ID，则必须要指定隧道名称，且指定的隧道名称的客户端才可以拨入。

# L2TP VPN故障排除步骤

- PPP验证模式不一致

查看拨号用户在客户端拨号工具中配置的PPP验证模式。

以VPN Client软件为例。如上图所示，PC客户端设置的隧道名称为“l2tp”，认证模式为“PAP”。

查看对应Virtual Template 使用的PPP认证模式。

```
<USG> system-view
[USG] interface Virtual-Template 99
[USG-Virtual-Template99] display this
 interface Virtual-Template99
ppp authentication-mode PAP
 ip address 99.99.99.24 255.255.255.0
 remote address pool 1
```








PPP认证有chap和pap，配置中注意属于哪一种认证。

# L2TP VPN故障排除步骤

- Virtual-Template接口未配置IP地址

  查看Virtual-Template接口信息，确认是否配置了IP地址。

```
<USG> system-view
[USG] interface Virtual-Template 99
[USG-Virtual-Template99] display this
#
 interface Virtual-Template99
ppp authentication-mode PAP
 ip address 99.99.99.24 255.255.255.0
 remote address pool 1
```






# L2TP VPN故障排除步骤

- Virtual-Template 接口视图下未指定正确的地址池

  在Virtual-Template接口视图下，确定是否指定了正确的地址池，根据对应的地 址池编号，查看AAA下的地址池是否配置成功。

```
<USG> system-view
[USG] interface Virtual-Template 99
[USG-Virtual-Template99] display this
#
 interface Virtual-Template99
ppp authentication-mode PAP
 ip address 99.99.99.24 255.255.255.0
 remote address pool 1
[USG] aaa
[USG-aaa] display this
 local-user admin password simple Admin@123
 ip pool 1 1.1.1.1 1.1.1.4
```






如果在Virtual-Template接口视图下未显示地址池，比如显示的是remote address pool，那么他默认调用的是地址池编号0。

# L2TP VPN故障排除步骤

- 地址池地址已分配完

  查看用户所在域引用地址池是否与对应Virtual Template引用地址池一致。

```
<USG> display ip pool domain abc
 ----------------------------------------------------------------------------------
Pool-number   Pool-start-addr   Pool-end-addr   Pool-length   Used-addr-number
 ----------------------------------------------------------------------------------
1             1.1.1.1           1.1.1.4         4             0
 ----------------------------------------------------------------------------------
Total pool number: 1
```



HUAWEI

Used-addr-number字段的值大于Pool-length字段的值，说明上线人数已经域最大用户接入数，需要等待当前L2TP客户下线后，修改域最大用户接入数。

Used-addr-number字段的值小于Pool-length字段的值，说明上线人数没有超过域最大用户接入数。



# 目录














# IPSEC VPN配置前需要准备的数据

- IKE协商的版本，目前包含IKEv1和IKEv2两种；
- 协商对端的IP地址，本端的IP地址，中间是否存在NAT的情况；
- 第一阶段的协商内容：协商模式（主模式、野蛮模式）、HASH算法（MD5、SHA1）、加密算法（DES、3DES、AES 128 | 192 | 256 ）、预共享密钥、DH-GROUP；
- 第二阶段的协商内容：IPSEC的封装协议（AH、ESP、AH+ESP）、认证算法（ MD5、SHA1 ）、加密算法（DES、3DES、AES 128 | 192 | 256 ）、PFS、需要保护的数据流。





# IPSEC VPN配置所遇到的问题（一）

- **ike和ipsec命令缺失**
  - 这是由于没有license的原因，需要购买了含有ipsec功能项license 并且通过license file xxx这个命令行导入了license才能执行ipsec 相 关命令行。可以通过display license来查看当前license所包含 ipsec 隧道数。
- **选择模板方式还是非模板方式**
  - 取决于对端设备特征，如果需要远程移动客户端接入，将不知道客户端IP地址，无法配置remote-address，只能使用模板方式，并且使用野蛮模式名字认证，如果是两个分支机构之间通信，IP 地 址是固定的，则使用非模板方式。





如果分支是不固定的ip，那么总部使用策略模板方式，分支使用子策略方式。

## IPSEC VPN配置所遇到的问题（二）

- 双机热备组网时，如何配置
  - 双机热备情况下，由于对端只配置本端的1个IP地址，所以本端必须使用虚IP作为IKE协商地址，可以在ipsec policy中配置local-address为对外虚IP。另外主备发生切换时，对端设备是无法马上感知的，所以需要对端设备支持DPD或keepalive，两 端都配置上DPD或keepalive。







- 使用ike dpd命令配置DPD功能时需要注意

如果指定interval参数，表示DPD工作在轮询模式，如果在DPD检测时间间隔内隧道中没有流量，则周期性发送DPD报文。

如果指定on-demand参数，表示DPD工作在流量触发模式，自上次流量结束时刻算起，如果在DPD检测时间间隔内隧道中没有流量，则只有在有发送流量时才会发送DPD报文，且DPD检测时间从零重新计算。否则隧道中不会有DPD报文。

如果没有指定interval或on-demand参数，DPD默认工作在流量触发模式。

- 配置Keepalive机制时需要注意

发送Keepalive报文的时间间隔和等待Keepalive报文的超时时间要成对出现，即在一个USG上配置了timeout参数，那么在对端就要配置interval参数。

在网络上一般不会出现超过连续三次的报文丢失，所以超时时间可以采用对端配置的Keepalive报文发送时间间隔的三倍。

interval的参数应该小于对端的timeout参数值，而不应该与本端进行比较。

# IPSEC配置问题快速诊断（一）

- 如果ike第一阶段无法建立
  - 1、2两个报文协商的是ike proposal 配置参数，如果发送第一个报文对端没有回应，需要检查两端设备ike proposal 配置参数是否一致；
  - 3、4两个报文协商的是key 、nonce，通常情况下如果1、2两个报文能通过，3、4报文一般不会有问题；
  - 5、6两个报文被加密，是ike peer 配置的身份 ip、psk等，如果对端没有回应，需要检查ike peer下配置参数与对端是否一致。





# IPSEC配置问题快速诊断（二）

- 如果ike阶段一建立成功，阶段二不成功
  - 第二阶段第一个报文发送的是ipsec proposal ，如果发送第一报文对端没有回应，检查设备两端ipsec proposal 参数配置是否一致；
  - 如果发送第一个报文，并收到第二个报文，但是没有回应报文3，或者收到报文2且回应了报文3但是隧道没有建立起来，可能是双方的感兴趣流量acl不匹配。








# 目录





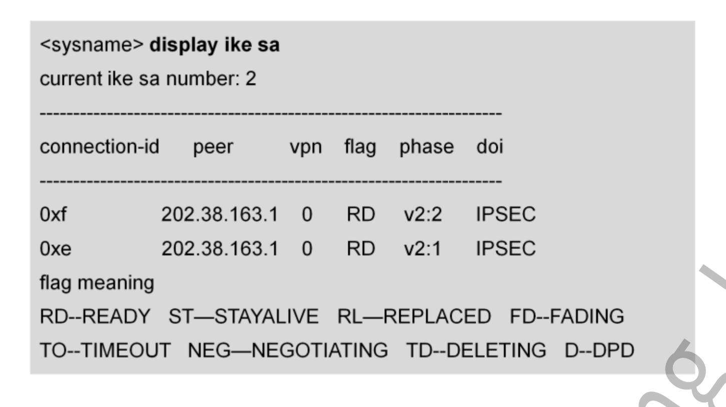






# IPSEC VPN故障排除相关命令（一）

- 显示所有IKE协商方式建立的安全联盟配置信息



```
<sysname> display ike sa
current ike sa number: 2
-----------------------------------------------------------------
connection-id     peer          vpn   flag   phase   doi
-----------------------------------------------------------------
0xf            202.38.163.1    0     RD     v2:2    IPSEC
0xe            202.38.163.1    0     RD     v2:1    IPSEC
flag meaning
RD--READY   ST—STAYALIVE   RL—REPLACED   FD--FADING
TO--TIMEOUT   NEG—NEGOTIATING   TD--DELETING   D--DPD
```








display ike sa命令输出信息描述：

current ike sa Num：IKE安全联盟的数量；

connection-id：安全通道的标识符；

Peer：此安全联盟的对端IP地址；

Vpn：VPN实例名称；

Flag：显示此安全联盟的状态：RD（READY）：表示此SA已建立成功； ST（STAYALIVE）：表示此端是通道协商发起方； RL（REPLACED）：表示此通道已经被新的通道代替，一段时间后将被删除； FD（FADING）：表示此通道已发生过一次软超时，目前还在使用，在硬超时时会删除此通道； TO（TIMEOUT）：表示此SA在上次keepalive超时发生后还没有收到keepalive报文，如果在下次keepalive超时发生时仍没有收到keepalive报文，此SA将被删除；

Phasem：此SA所属阶段：Phase 1：建立安全通道进行通信的阶段，此阶段建立ISAKMP SA；Phase 2：协商安全服务的阶段，此阶段建立IPSec SA；

Doi：SA所属解释域。

# IPSEC VPN故障排除相关命令（二）

- 显示所有安全联盟的配置信息

```
<sysname> display ipsec sa
```

- 查看IPSec报文统计信息

```
<sysname> display ipsec statistics
the security packet statistics:
input/output security packets: 4/4
input/output security bytes: 400/400
input/output dropped security packets: 0/0
```







display ipsec statistics命令输出信息描述：

input/output security packets：受安全保护的输入/输出数据包；

input/output security bytes：受安全保护的输入/输出字节数；

input/output dropped security packets：被丢弃受安全保护的输入/输出数据包。

# IPSEC VPN故障排除相关命令（三）

- 详细IPSec报文的统计信息注释

```
<USG>display  ipsec  statistics
the security packet statistics:
  input/output security packets: 4/4                    收到/发送的ipsec报文数
  input/output security bytes: 400/464                  收到/发送的ipsec字节数
  input/output dropped security packets: 0/0            被丢弃的收到/发送报文数，详细信息见下
面统计
  dropped security packet detail:
    no enough memory: 0                                 没有内存而丢包，一般不会发生
    can't find SA: 0                                    找不到sa而丢包，可能sa没协商好
    queue is full: 0                                    队列满而丢包，一般不会发生
    authentication is failed: 0                         验证失败而丢包很少发生，如果有可能是
伪造的报文，或者对端设备问题
```





# IPSEC VPN故障排除相关命令（四）

- 详细IPSec报文的统计信息注释(续)

| | |
|---|---|
| wrong length: 0 | 错误的长度而丢包，很少发生 |
| replay packet: 0 | 重放报文，中间设备抓包重放导致，或者两端的设备处理序列号的机制不同步导致 |
| too long packet: 0 | 过长的报文而丢包，很少发生 |
| wrong SA: 0 | 错误的sa，可能sa没协商好，或者两端的sa不一致 |
| encry fail: 0 | 加密错误，很少发生 |
| decry fail: 0 | 解密错误，很少发生 |
| check acl car: 0 | 对已经发起协商的流的报文的丢弃 |
| speed limit car: 0 | 协商速率的限制 |
| pre-check fail: 0 | 前反查丢包，收到需要加密但没加密的报文，说明对端设备配置或处理问题 |
| succeed-check fail: 0 | 反查解密后的报文，不符合配置的acl |
| other reasons: 0 | 其他错误，很少发生 |







# IPSEC VPN故障排除相关命令（五）

- 重要debug信息注释
  - ike propsal配置不一致，包括加密算法、HASH算法、DH算法等，需要打开debugging ike error。

```
对端发起协商，本端会打印如下信息：
2011-06-07 14:38:36 USG %%01IKE/4/WARNING(l): phase1: proposal mismatch, please check
ike proposal configuration.
0.508983 USG %%01IKE/7/DEBUG(d): dropped message from 3.3.3.1 due to notification type
NO_PROPOSAL_CHOSEN
```

```
本端发起协商，对端拒绝时，可能会打印如下信息，但如果对端不会发送协商失败的notify消息，
则不会打印：
2011-05-23 20:38:48 Eudemon %%01IKE/4/WARNING(l): phase1: proposal mismatch, ple
ase check ike proposal configuration.
0.591250 Eudemon %%01IKE/7/DEBUG(d): got NOTIFY of type NO_PROPOSAL_CHOSEN
```






# IPSEC VPN故障排除相关命令（六）

- 重要debug信息注释
  - ipsec propsal配置不一致，包括加密算法、认证算法、DH算法等，需要打开debugging ike error。

```
对端发起协商，本端会打印如下信息：
2011-06-08 19:00:06  %%01IKE/4/WARNING(l): phase2: proposal mismatch, ple
ase check ipsec proposal configuration.
0.34476900  %%01IKE/7/DEBUG(d): dropped message from 3.3.3.1 due to notif
ication type NO_PROPOSAL_CHOSEN
```

```
本端发起协商，对端拒绝时，可能会打印如下信息，但如果对端不会发送协商失败的notify消息，
则不会打印：
2011-05-25 00:58:46 USG %%01IKE/4/WARNING(l): phase2: proposal mismatch, ple
ase check ipsec proposal configuration.
0.34481316 Eudemon %%01IKE/7/DEBUG(d): got NOTIFY of type NO_PROPOSAL_CHOSEN
```





# IPSEC VPN故障排除相关命令（七）

- 重要debug信息注释
  - acl配置不一致，需打开debugging ike misc和debugging ike error 。

打开debugging ike error查看对端发过来的acl，打印的内容会比较多，找到如下内容，即对端发送来的acl，但已经将源和目的对调了，只要直接和本地比较就行。

0.35223783 USG %%01IKE/7/DEBUG(d): proid:0
0.35223850 USG %%01IKE/7/DEBUG(d): src addr:0x03030300 mask:0xFFFFFF00
0.35223933 USG %%01IKE/7/DEBUG(d): src port:0
0.35224000 USG %%01IKE/7/DEBUG(d): dst addr:0x03030300 mask:0xFFFFFF00
0.35224083 USG %%01IKE/7/DEBUG(d): dst port:0

如果匹配不对，响应端会打印如下信息：

2011-06-08 19:18:01 USG %%01IKE/4/WARNING(l): phase2: security acl mismatch.

发起端acl匹配错误，可能会打印如下信息（只要开启debugging ike error）：

2011-05-25 01:16:40 Eudemon %%01IKE/4/WARNING(l): phase2: security acl mismatch.
0.35555900 Eudemon %%01IKE/7/DEBUG(d): got NOTIFY of type INVALID_ID_INFORMATION








# 目录













# IPSec VPN故障排除：网关对网关

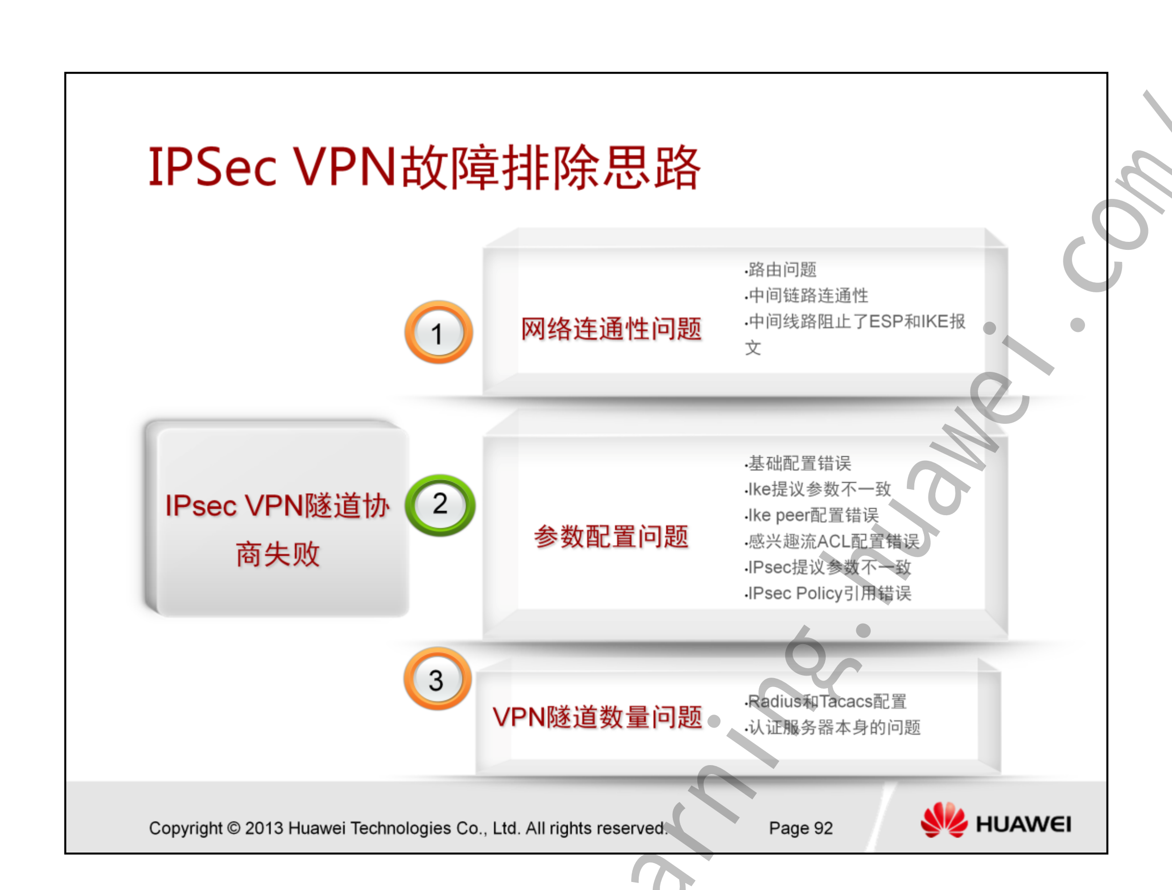



- 现象描述
  - 2个LAN之间进行资源传输，当使用IKE方式建立IPSec隧道时，协商失败。
- 可能原因
  - 原因一：连通性问题。
  - 原因二：配置问题。
  - 原因三：VPN隧道数量问题。



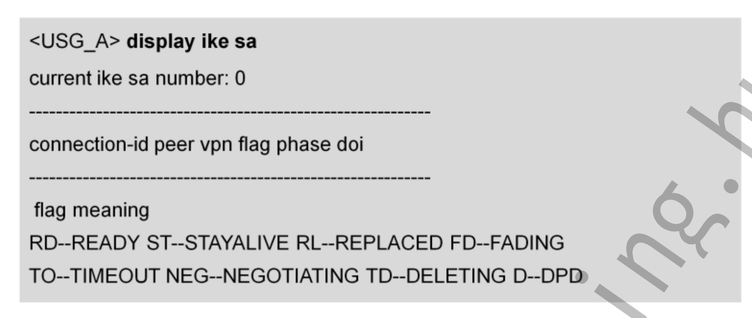





IPSec VPN故障排除思路
IPsec VPN隧道协商失败
1
网络连通性问题
·路由问题
·中间链路连通性
·中间线路阻止了ESP和IKE报文
2
参数配置问题
·基础配置错误
·Ike提议参数不一致
·Ike peer配置错误
·感兴趣流ACL配置错误
·IPsec提议参数不一致
·IPsec Policy引用错误
3
VPN隧道数量问题
·Radius和Tacacs配置
·认证服务器本身的问题
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 92
HUAWEI

# IPSec VPN故障排除步骤（一）

- 在PC A上ping PC B，然后在USG_A执行display ike sa命令，查看安全联盟建立情况。
  - 若没有建立任何安全联盟，说明第一阶段安全联盟建立失败。显示信息 如下所示。



```
<USG_A> display ike sa
current ike sa number: 0
-----------------------------------------------------------
connection-id peer vpn flag phase doi
-----------------------------------------------------------
 flag meaning
RD--READY ST--STAYALIVE RL--REPLACED FD--FADING
TO--TIMEOUT NEG--NEGOTIATING TD--DELETING D--DPD
```



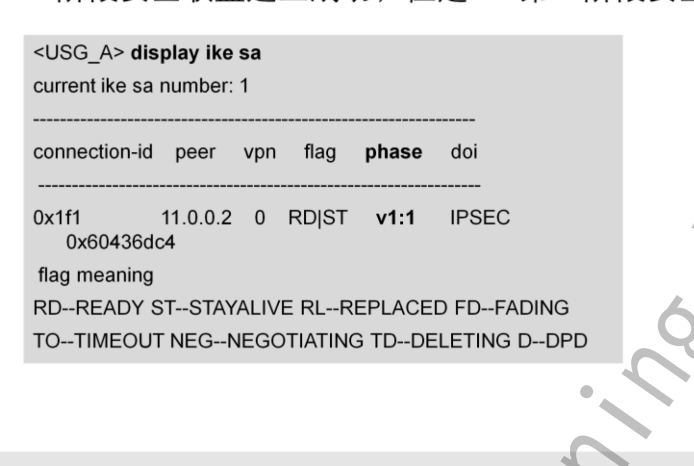




第一阶段安全联盟建立失败的情况下，重点请排查原因一和原因三。

## IPSec VPN故障排除步骤（二）

- 若建立安全联盟phase字段值只包括v1:1或v2:1，说明IKE第一阶段安全联盟建立成功，但是IKE第二阶段安全联盟建立失败



```
<USG_A> display ike sa
current ike sa number: 1
---------------------------------------------------------------------
connection-id   peer   vpn   flag   phase   doi
---------------------------------------------------------------------
0x1f1          11.0.0.2   0   RD|ST   v1:1   IPSEC
     0x60436dc4
flag meaning
RD--READY ST--STAYALIVE RL--REPLACED FD--FADING
TO--TIMEOUT NEG--NEGOTIATING TD--DELETING D--DPD
```







第一阶段安全联盟建立成功但第二阶段安全联盟建立失败的情况下，重点请排查原因二。

## IPSec VPN故障排除步骤（三）

- 原因一：连通性问题
  - 路由问题：PC没有到对端内网路由；防火墙没有到PC路由和到对端防火墙出口路由不可达；
  - 中间链路问题：比如中间线路接口、线缆故障、设备路由等；
  - 中间设备阻止IKE报文和ESP报文。
- 原因二：配置问题
  - 基本配置错误：执行**display ip interface brief**命令，查看接口是否正确配置IP地址、域间包过滤等基本配置错误。





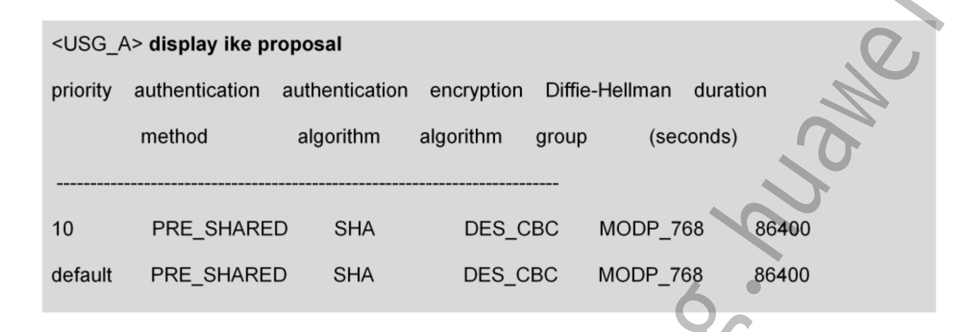


ike报文使用udp的500端口。未开启nat穿越情况下，AH和ESP直接通过IP承载，协议号分别为51和50。开启nat穿越情况下，ESP使用udp的4500端口。所以需要检查中间设备是否阻止协议号为51和50以及udp500和4500端口的报文通过。

# IPSec VPN故障排除步骤（四）

- IKE安全提议不一致

  在USG_A上执行display ike proposal命令，查看相应IKE安全提议配置。



```
<USG_A> display ike proposal
priority  authentication  authentication  encryption  Diffie-Hellman  duration
           method          algorithm       algorithm   group          (seconds)
------------------------------------------------------------------------
10        PRE_SHARED      SHA             DES_CBC     MODP_768       86400
default   PRE_SHARED      SHA             DES_CBC     MODP_768       86400
```








可以看出USG_A上，IKE安全提议号为10，采用的验证方法为预共享方法（PRE_SHARED），验证算法为SHA，加密算法为DES，生存周期为86400s。

在USG_B上执行display ike proposal命令，查看相应IKE安全提议的配置。

比较USG_A与USG_B上的IKE安全提议的配置是否一致。若不一致请修改为一致。

# IPSec VPN故障排除步骤（五）

- IKE Peer配置错误

  在USG_A上执行display ike peer name peer-name命令，查看IKE对等体配置是否正确。

```
<USG_A> display ike peer name a
---------------------------
IKE Peer: a
  exchange mode: main on phase 1
  pre-shared-key: gateway
  certificate domain name:
  certificate file name:
  proposal: 10
  local id type: ip
  peer ip address: 11.0.0.2
  nat traversal: disable
  applied to 1 policy: pol-1-isakmp
```







从上图可以看出USG_A IKE Peer名称为a，第一阶段IKE的协商模式为主模式，预共享密钥设置为gateway，本地ID类型为IP方式，对端IP地址为11.0.0.2，不开启NAT穿越功能，应用到安全策略名称为pol，序号为1的IPSec安全策略中。

USG_B，display ike peer name peer-name命令查看相应IKE对等体配置是否正确。

比较USG_A与USG_B配置，查看配置是否正确。包括协商方式是否一致，预共享密钥是否一致，对端IP地址是否正确。

说明：若两网关中间存在NAT设备，需要开启NAT穿越。

## IPSec VPN故障排除步骤（六）

- 感兴趣流量ACL配置错误

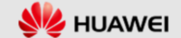
在USG_A上执行display acl acl-number命令，查看安全策略所引用ACL规则配置是否正确。

```
[USG_A] display acl 3001
Advanced ACL 3001, 1 rule,not binding with vpn-instance
Acl's step is 5
rule 5 permit ip source 10.0.0.0 0.0.0.255 destination 10.0.1.0 0.0.0.255
```

在USG_B上执行display acl acl-number，查看安全策略所引用ACL规则配置是否正确。

```
[USG_B] display acl 3001
Advanced ACL 3001, 1 rule,not binding with vpn-instance
Acl's step is 5
rule 5 permit ip source 10.0.1.0 0.0.0.255 destination 10.0.0.0 0.0.0.255
```




- 建议两端配置的ACl规则互为镜像。配置为镜像不是必要条件，不过实际应用中配置成镜像更简单也不易出错。

  一般来讲，只要发起方配置的ACL规则范围比响应方小就可以。对于IKEv2来说，双方ACL规则取交集。

- 对于特殊组网的感兴趣流量ACL配置为:

  l2tp over ipsec LNS端感兴趣流量ACL配置

  例如： acl number 3001

  rule 0 permit udp source 202.134.20.15 0 source-port eq 1701

  //匹配源地址为外网口地址，源端口为udp1701的流量。

  gre over ipsec感兴趣流量ACL配置

  例如：acl number 3001

  rule 0 permit ip source 202.134.20.15 0 destination 128.78.56.3 0

  //该组网的感兴趣流量acl和普通网关对网关的acl写法一样，只是里面的网段不再是私网，而是公网出口的网段。

  同时开启ipsec和nat outboud的感兴趣流量ACL配置

  该组网的感兴趣流量acl和普通的网关对网关的acl写法一样，只是在nat outbound所对应的acl（或者nat-policy）里把走vpn的网段优先deny掉。

# IPSec VPN故障排除步骤（七）

- IPSec安全提议不一致

在USG_A上执行display ipsec proposal name proposal_name命令，查看IPSec安全提议配置。

```
[USG_A] display ipsec proposal name pro
IPsec proposal name: pro
encapsulation mode: tunnel
transform: esp-new
ESP protocol: authentication md5-hmac-96, encryption des
applied to policies: pol-1-isakmp
```








可以看出在USG_A上，IPSec安全提议的名称为pro，采用的报文封装模式为隧道模式，安全协议采用esp协议，esp协议采用的认证算法为MD5，采用的加密算法为DES。该安全提议应用到安全策略名称为pol，序号为1的IPSec安全策略中

在USG_B上执行display ipsec proposal name proposal_name命令，查看IPSec安全提议的配置。

比较USG_A与USG_B配置，查看配置是否一致。

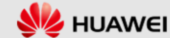
# IPSec VPN故障排除步骤（八）

- IPSEC policy安全策略引用错误

在USG_A上执行display ipsec policy name policy_name命令，查看IPSec安全 策略配置。

```
[USG_A] display ipsec policy name pol
IPsec Policy Group: "pol"
Using interface: {}
-----------------------------
IPsec policy name: "pol"
sequence number: 1
mode: isakmp
 -----------------------------
security data flow : 3001
ike-peer name: a
perfect forward secrecy: None
proposal name: pro
IPsec sa local duration(time based): 3600 seconds
IPsec sa local duration(traffic based): 1843200 kilobytes
```




从上图可以看出在USG_A上，建立的安全策略组名称为pol，pol序号为1的安全策略，引用了名称为a的IKE Peer和名称为pro的IPSec安全提议以及ACL 3001规则组。

在USG_B上执行display ipsec policy name policy_name命令，查看IPSec安全策略的配置。

比较USG_A与USG_B上的配置，查看配置是否一致。 若不一致请修改为一致。

# IPSec VPN故障排除步骤（九）

- 原因三：**VPN隧道数量问题**
  - 无IPSec VPN license；
  - VPN隧道数量已满。








# 目录

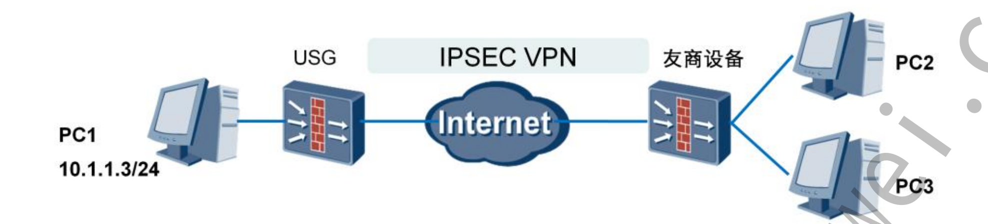








# 案例1：异构设备导致IPSec VPN不通




- 故障描述
  - 组网如图1所示，通过一台USG与一台友商设备建立IPSec VPN。IPSec VPN建立以后，PC1可以ping通PC2，但无法ping通PC3，IKE阶段1建立成功，PC1和PC2之间的IKE阶段2和IPSec SA建立成功，PC1和PC3之间的IKE阶段2和IPSec SA建立失败。



# 案例1：异构设备导致IPSec VPN不通

- 处理过程
  - 在PC3上执行tracert 10.1.1.3;
  - 可tracert到友商设备，说明PC3与友商设备之间路由可达;
  - 检查友商设备设备本地地址列表配置，确认包含PC3 IP地址;
  - 在USG上将ACL规则组拆分成多个ACL规则组，每个ACL规则组内只配置一条规则，再配置一个IPSec策略组包括多条IPSec策略。





由于USG一个ACL规则组对应一个IPSec隧道，但是有的友商设备尽管access-list可以配置多条规则，但是一条规则对应一个IPSec隧道。这样就会导致ACL配置多条规则时，只有发起协商的那个规则对应的数据流能通，其它规则的数据流均不通。碰到这种情况时，需要配置多个ACL，每个ACL配置一条规则，再使用配置同一策略组下的多条策略的方式。

# 案例1：异构设备导致IPSec VPN不通

```
acl number 3020
 rule 5 permit ip source 10.196.226.7 0 destination 172.31.16.200 0
 #
acl number 3021
 rule 5 permit ip source 10.196.226.7 0 destination 172.31.14.2 0
#
ipsec policy map 20 isakmp
   security acl 3020
   ike-peer ufone
   proposal sha
#
ipsec policy map 21 isakmp
  security acl 3021
  ike-peer ufone
  proposal sha
```





# 案例2：IPSec主动建立隧道失败




- 故障描述
  - USG设备和对端友商设备建立ipsec vpn隧道。从友商设备触发隧道可以正常建立成功，从USG设备主动发起隧道协商不成功。






对于udp报文需用户调整pc或服务器网卡mtu。

# 案例2：IPSec主动建立隧道失败

- 原因分析
  - 不能主动发起侧的策略是模板方式。对于这种情况属正常现象，无需处理；
  - 一端仅支持IKEv1（不支持IKEv2），另一端支持IKEv1和IKEv2。





# 案例2：IPSec主动建立隧道失败

- 处理过程
  - 两端设备都是采用子策略方式，而友商设备仅支持IKEv1；
  - USG设备能够自适应地支持IKEv1和IKEv2，默认情况下使用IKEv2，而友商设备只支持IKEv1；
  - 如果友商设备先发起IKE协商且使用IKEv1，USG设备可自适应地响应IKEv1或IKEv2协商，故可以建立起协商。当USG设备主动发起协商时，默认使用IKEv2进行协商，将使对端设备无法响应IKEv2协商，导致隧道建立不起来；
  - 在USG设备ike peer视图下，输入命令undo version 2，问题解决。







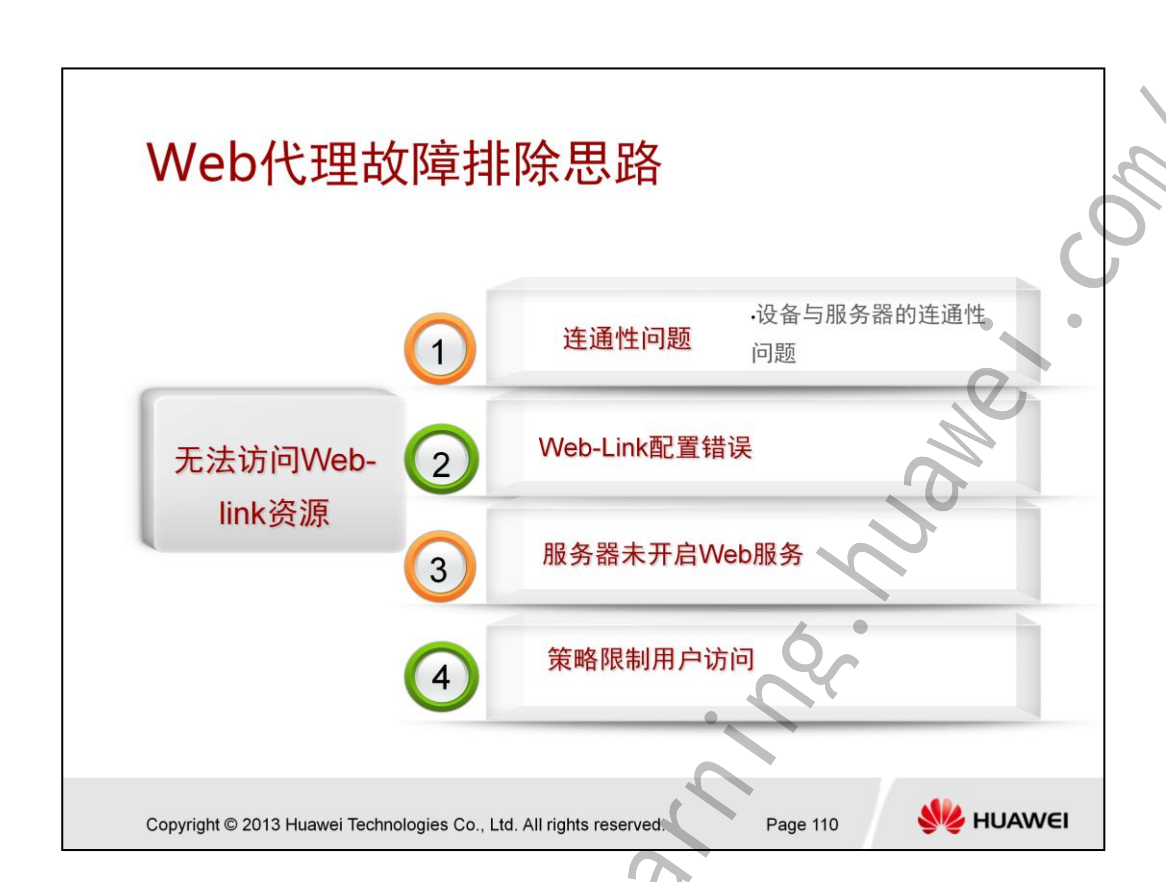
# 目录











Web代理故障排除思路
无法访问Web-link资源
1
连通性问题
·设备与服务器的连通性问题
2
Web-Link配置错误
3
服务器未开启Web服务
4
策略限制用户访问
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 110
HUAWEI

# Web代理故障排除步骤（一）

- 原因一：连通性问题
  - 在USG上使用ping命令ping内网服务器IP地址，检查网络连接。如果ping不通，则说明虚拟网关和内网服务器之间路由存在问题或接口、线路有故障问题。
- 原因二：**web-link**配置问题
  - 若WEB服务器下级目录打不开，是由于下级目录链接不在web-link配置里。






# Web代理故障排除步骤（二）

- 原因三：内网服务器未开启**Web**服务
  - 在内网服务器上执行netstat -anp tcp命令，查看Web服务端口是否正在侦听（LISTENING）。若没有侦听请检查Web服务。
- 原因四：策略限制用户访问
  - 检查虚拟网关策略设置，可能是由于策略设置限制该用户对这条资源访问权限，请修改相关策略规则设置。







# 目录



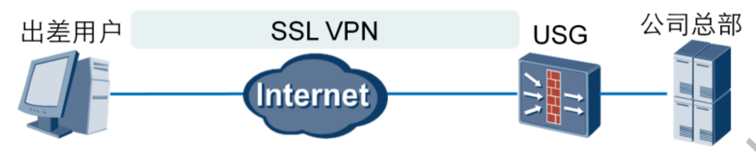








# 网络扩展故障排除

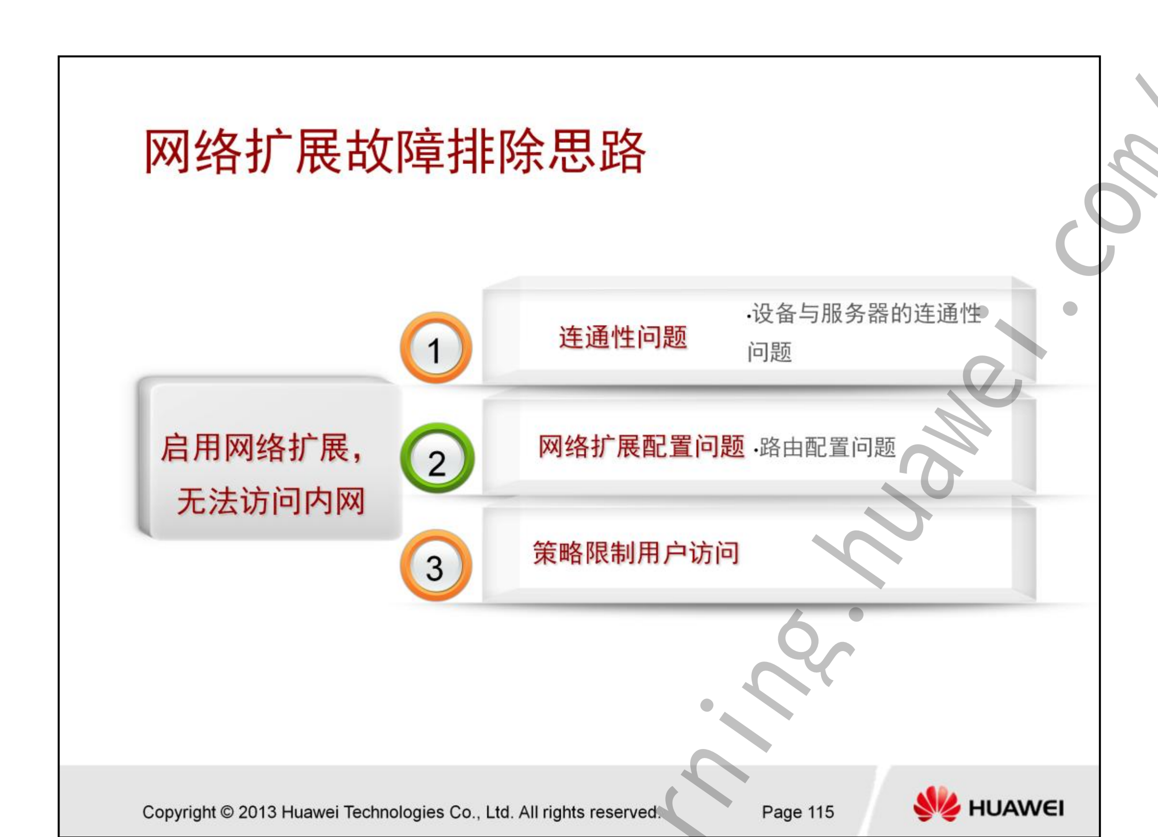



- 现象描述
  - 用户在PC上启用网络扩展，已获得分配的地址。用户PC不能使用网络扩展业务访问内网服务器的资源。
- 可能原因
  - 原因一：连通性问题；
  - 原因二：网络扩展配置问题；
  - 原因三：策略限制用户访问。





如果访问的资源为域名形式，那么还需要检查虚拟网关的DNS服务器是否配置正确。


网络扩展故障排除思路
启用网络扩展，
无法访问内网
1
连通性问题
·设备与服务器的连通性
问题
2
网络扩展配置问题
·路由配置问题
3
策略限制用户访问
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 115
HUAWEI

# 网络扩展故障排除步骤（一）

- 原因一：连通性问题
  - USG上没有配置到内网服务器的路由；
  - 内网服务器上没有到网络扩展虚拟IP地址的路由；
  - USG和内网服务器之间的路由设备上没有配置到网络扩展虚拟IP地址的路由；
  - 中间链路问题或访问限制。





# 网络扩展故障排除步骤（二）

- 原因二：网络扩展配置问题
  - 如果客户端路由方式为“分离模式”或“全路由模式”，可以排除这个原因，请查看原因三继续排除故障；
  - 如果客户端路由方式为“手动模式”，请检查是否配置了服务器的IP网段，如果没有，请添加。






路由方式查看方法：

在“菜单”导航树中选择“VPN > SSL VPN”；

选择“虚拟网关列表”页签；

在“虚拟网关列表”导航树中选择“虚拟网关列表 > 虚拟网关名称 > 网络扩展”；

检查客户端路由方式。

# 网络扩展故障排除步骤（三）

- 原因三：策略限制用户访问
  - 在“虚拟网关列表”导航树中选择“虚拟网关列表 > 虚拟网关名称 > 策略 配置 > 用户策略”，查看该用户的目的IP型策略是否限制该用户访问内网服务器资源。如果有，请删除；
  - 选择“组策略”，查看该用户所属组的目的IP型策略是否限制访问内网服务器资源。如果有，请删除；
  - 在“虚拟网关列表”导航树上单击“网络扩展”，查看该用户是否已经启用网络扩展。如果没有启用，请启用网络扩展功能。







# 目录










端口转发故障排除思路
无法访问端口转发资源
1
连通性问题
2
端口转发控件未启用或者未安装
3
用户连接超时
4
内网服务器没有开启相应的端口
5
策略限制用户访问该资源
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 120
HUAWEI

## 端口转发故障排除步骤（一）

- 原因一：连通性问题
  - 在USG上ping内网服务器，查看是否可以ping通。
- 原因二：端口转发未启用
  - 用户登录虚拟网关页面，若“端口转发”栏按钮上文字为“启动”，则表示未启动端口转发，请单击“启动”启动端口转发。
- 原因三：用户连接超时
  - 用户连接超时后，“端口转发”栏按钮上文字变为“启动”，请单击“启动” 重新启动端口转发。如果单击“启动”，界面跳回登录页面，请重新登录并启动端口转发。






端口转发业务正常启用后，“端口转发”栏下的按钮上的文字会由“启动”变为“关闭”。当关闭端口转发业务或用户与虚拟网关断开连接后，会恢复为“启动”。

## 端口转发故障排除步骤（二）

- 原因四：内网服务器没有开启相应的服务
  - 在内网服务器上执行netstat -an命令，查看该服务端口是否正在侦听（LISTENING），如果没有侦听请检查相应服务。
- 原因五：策略限制用户访问该资源
  - 在“虚拟网关列表”导航树中选择“虚拟网关列表 > 虚拟网关名称 > 端口转发”，查看该虚拟网关是否已经启用端口转发并关联端口转发资源。如果没有请启用端口转发并关联端口转发资源。






当端口转发资源配置为any IP时，有时用户可以在页面上看到无法访问的资源。例如，配置了一条资源，使用户A可以访问所有内网服务器上的80端口资源。同时，管理员添加一条策略规则：限制用户访问服务器B上的80端口资源，那么用户仍然能看到该端口转发资源，但无法访问服务器B上的80端口资源（其他服务器上的资源可正常访问）。



# 目录








## 文件共享故障排除

- 现象描述
  - 在虚拟网关上启用了文件共享业务，并配置了文件共享资源。用户登录虚拟网关，成功访问配置文件共享资源，但只能查看目录和文件，无法进行文件上传、删除或重命名等操作。
- 可能原因
  - 原因一：如果文件服务器类型为NFS，说明用户UID和GID属性不允许用户进行上传、删除或重命名文件的操作；
  - 原因二：如果文件服务器类型为SMB，当前登录用户对该文件共享资源只具有读操作权限，而没有写操作权限。






NFS文件服务器根据登录用户的UID和GID进行资源访问的权限控制，NFS类型的共享文件可设置三种用户群：

拥有者

拥有者即为共享文件的创建者。

同组用户

同组用户与拥有者的GID相同，但UID不同。

其他用户

其他用户的GID、UID与拥有者的GID、UID均不同。

这三种用户群的文件权限可以设为不同，说明用户根据UID和GID归类到相应的用户群以访问文件。

# 文件共享故障排除步骤

- 原因一：如果文件服务器类型为NFS，用户UID和GID属性不允许用户进行上传、删除或重命名文件的操作。
  - 在“虚拟网关列表”导航树中选择“虚拟网关列表 > 虚拟网关名称 > VPNDB配置”， 选择相关用户，将用户UID、GID设置为NFS文件服务器上具有该目录写权限的UID、GID。

- 原因二：如果文件服务器类型为SMB，当前登录用户对该文件共享资源只具有读操作权限，而没有写操作的权限。
  - 请联系文件服务器管理员，为该用户申请写操作权限。







# 总结

- 安全策略常见故障及排除方法
- 基于源和基于目的的NAT转换的常见故障及排除思路
- IP-Car常见故障及排除思路
- DPI常见故障排除及思路
- 双机热备常见故障及排除思路
- L2TP VPN常见故障及排除思路
- IPSEC VPN常见故障及排除思路
- GRE VPN常见故障及排除思路
- SSL VPN的故障排除及思路








# 思考题

- 安全策略常见故障及排除方法?
- 基于源和基于目的的NAT转换的常见故障及排除思路?
- IP-Car常见故障及排除思路?
- DPI常见故障排除及思路?
- 双机热备常见故障及排除思路?
- L2TP VPN常见故障及排除思路?
- IPSEC VPN常见故障及排除思路?
- GRE VPN常见故障及排除思路?
- SSL VPN的故障排除及思路?






## 练习题

- 判断题
  1. Virtual-Template接口若未加入到安全区域，L2TP VPN拨号将不能成功。
- 单选题
  1. 控制台打印信息如下，说法正确的有?

  2011-06-08 19:00:06 %%01IKE/4/WARNING(l): phase2: proposal mismatch, please check ipsec proposal configuration.

  0.34476900 %%01IKE/7/DEBUG(d): dropped message from 3.3.3.1 due to notification type NO_PROPOSAL_CHOSEN

  A、两端的ike提议不匹配 B、两端的ipsec提议不匹配

  C、由本端发起协商 D、由对端发起协商






习题与答案：

1、Virtual-Template接口若未加入到安全区域，L2TP VPN拨号将不能成功。

答案：错误

2、控制台打印信息如下，说法正确的有?

2011-06-08 19:00:06 %%01IKE/4/WARNING(l): phase2: proposal mismatch, please check ipsec proposal configuration.

0.34476900 %%01IKE/7/DEBUG(d): dropped message from 3.3.3.1 due to notification type NO_PROPOSAL_CHOSEN

A、两端的ike提议不匹配

B、两端的ipsec提议不匹配

C、由本端发起协商

D、由对端发起协商

答案：B|D



# 练习题

- 判断题

  1. 配置nat server时添加no-reverse参数后，需要配置 nat outbound，inside 地址才能回应报文。

- 单选题

  1. 下列关于ip-car白名单说法正确的有？

  A、命中permit规则将不进行限流

  B、命中deny规则将不进行限流

  C、白名单比限流策略先匹配

  D、白名单比限流策略后匹配









习题与答案：

1、配置nat server时添加no-reverse参数后，需要配置 nat outbound，inside地址才能回应报文。

答案：错误

2、下列关于ip-car白名单说法正确的有？

A、命中permit规则将不进行限流

B、命中deny规则将不进行限流

C、白名单比限流策略先匹配

D、白名单比限流策略后匹配

答案：B|C

Thank you

www.huawei.com

# 华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*) 享有如下特权：

- **1、华为E-learning 课程学习**
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：请提交您的“华为账号”和注册账号的“email地址”到 *Learning@huawei.com 申请权限。*
- **2、华为培训教材下载**
  - **内容**：**华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训->面授培训*”，在具体课程页面即可下载教材。
- **3、华为在线公开课(LVC)优先参与**
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见LVC排期：
    http://support.huawei.com/learning/NavigationAction!createNavi#navi[id]=_16
- **4、学习工具 eNSP**
  - *eNSP (Enterprise Network Simulation Platform)*，是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。（http://support.huawei.com/ecommunity/bbs/list_2247.html ）